Advanced Software Protection:
Integration, Research and Exploitation

D7.05

Dissemination Report

Project no.:	609734
Funding scheme:	Collaborative project
Start date of the project:	1st November 2013
Duration:	36 months
Work programme topic:	FP7-ICT-2013-10
Deliverable type:	Report
Deliverable reference number:	ICT-609734 / D7.05 / 1.01
WP and tasks contributing:	WP 7 / Tasks 7.1
Due date:	October 2016, M36
Actual submission date:	9 December 2016
Responsible Organization:	UEL
Editor:	Paolo Falcarin, Elena Gómez-Martínez
Dissemination Level:	Public
Revision:	1.1

Abstract:

In collaborative research projects with partners from research and industry, dissemination of results plays a major role. In this report, we present all the activities undertaken during the project to spread the research results in the industrial and scientific community.

Keywords: website, presentations, poster, leaflet, logo, workshops, publications, tutorials, press release

Editor

Paolo Falcarin, Elena Gómez-Martínez (UEL)

Contributors (ordered according to beneficiary numbers)

Bjorn De Sutter (Ugent)

Cataldo Basile (POL)

Brecht Wyseur (NAGRA)

Mariano Ceccato (FBK)

Paolo Falcarin, Elena Gómez-Martínez (UEL)

The ASPIRE Consortium consists of:

Ghent University (UGent)	Coordinator & Beneficiary	Belgium
Politecnico Di Torino (POLITO)	Beneficiary	Italy
Nagravision SA (NAGRA)	Beneficiary	Switzerland
Fondazione Bruno Kessler (FBK)	Beneficiary	Italy
University of East London (UEL)	Beneficiary	UK
SFNT Germany GmbH (SFNT)	Beneficiary	Germany
Gemalto SA (GTO)	Beneficiary	France

Coordinating person:	Prof. Bjorn De Sutter
E-mail:	coordinator@aspire-fp7.eu
Tel:	+32 9 264 3367
Fax:	+32 9 264 3594
Project website:	www.aspire-fp7.eu

Disclaimer
The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 609734.
The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Executive Summary

This report lists and details the dissemination activities undertaken by the consortium partners during the project. These activities can be summarized as follows:

- a project logo;
- a Word and LaTex document templates
- a PowerPoint presentation template
- a 4-page A4 project leaflet;
- an A0 project poster;
- a project website
- social media activities (LinkedIn, Twitter);
- an open source repository;
- 25 scientific publications (of which 17 peer-reviewed);
- 18 participation activities in Conference or Workshops;
- 35 presentation activities where ASPIRE results were disseminated to expert audiences;
- 30 demonstration movies on YouTube;
- Organization of 2 international workshops on software protection, co-located with top conferences (ICSE-2015 and CCS-2016);
- 11 dissemination activities to the general public, including press releases taken up by ACM TechNews, and an interview with the coordinator broadcasted on Flemish local public television at the time of the project kick-off meeting.

Document History

In v1.1, one additional peer reviewed publication was added (nr. 17 on page 17 in Section 3.1).

Contents

Section 1 Dissemination Materials 1

1.1 Project Logo 1

1.2 Templates 1

1.3 Project Leaflet 2

1.4 Project Poster 7

Section 2 Online Presence 8

2.1 ASPIRE Project Website 8

2.1.1 Public ASPIRE Website http://www.aspire-fp7.eu 8

2.1.2 Restricted Area of ASPIRE Website 15

2.2 Social Media 15

2.3 YouTube Channel 15

2.4 Open Sourcing 15

Section 3 Scientific Publications 17

3.1 Peer-reviewed publications 17

3.2 Other publications (non peer-reviewed) 18

Section 4 Face-to-Face Dissemination 20

4.1 Participations in Conference or Workshops 20

4.2 Presentations 23

4.3 Upcoming Events 28

Section 5 Workshops 30

5.1 1st International Workshop on Software PROtection 30

5.2 2nd International Workshop on Software PROtection 33

Section 6 Public General Dissemination 36

6.1 Web, Press Releases, Articles in Popular Press, TV Footage 36

Section 7 Cooperation with Other Projects 40

7.1 Activities 40

Section 8 List of Abbreviations 41

List of Figures

Figure 1 - ASPIRE logo 1
Figure 2 - ASPIRE buttons 1
Figure 3 - Examples of ASPIRE presentation template 2
Figure 4 - Front page ASPIRE leaflet 3
Figure 5 - Page 2 ASPIRE leaflet 4
Figure 6 - Page 3 ASPIRE leaflet 5
Figure 7 - Back page ASPIRE leaflet 6
Figure 8 - ASPIRE poster 7
Figure 9- Screenshot of the top part of the home page on the ASPIRE website 10
Figure 10 - Screenshot of the ASPIRE website home page on an iPhone 3G. 10
Figure 11 - Screenshot of the consortium page on the ASPIRE website 11
Figure 12 - Screenshot of the contact form on the ASPIRE website.....................................11
Figure 13- Screenshot of the publications page on the ASPIRE website 12
Figure 14- Screenshot of knowledge base page on the ASPIRE website 12
Figure 15 - Screenshot of the ASPIRE webpage with the list of deliverables 13
Figure 16 - Unique users per country visiting the ASPIRE website (June 2014 - Nov 2016).14
Figure 17- The First SPRO website banner. 30
Figure 18 - The SPRO'16 banner 33
Figure 19 - Screenshot local television interview/report on AVS 38
Figure 20 - Screenshot local television report on TGVerona 38

List of Tables

Table 1: Google Analytics from ASPIRE website 14

Section 1 Dissemination Materials

Section Authors:

Bjorn De Sutter (UGent)

1.1 Project Logo

To allow for a head start of the dissemination activities, the project coordinator launched a design contest "Create the next logo for ASPIRE" at the online design contest marketplace 99designs.com on 18 Sep 2013. In a process that lasted three weeks, 355 designs were submitted by about 40 designers. Initially the coordinator provided feedback on submitted designs himself, in later phases the ASPIRE Steering Board joined the selection process.

Eventually, the logo depicted in Figure 1 was selected:

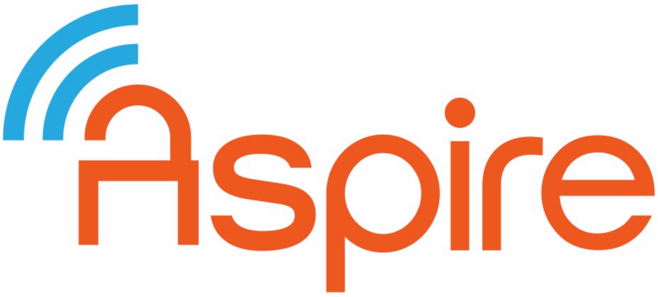


Figure 1 - ASPIRE logo

Along with that logo, the two buttons depicted in Figure 2 were delivered that can be used in all kinds of graphical dissemination material.

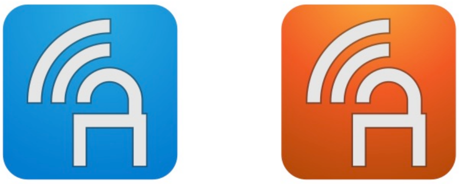
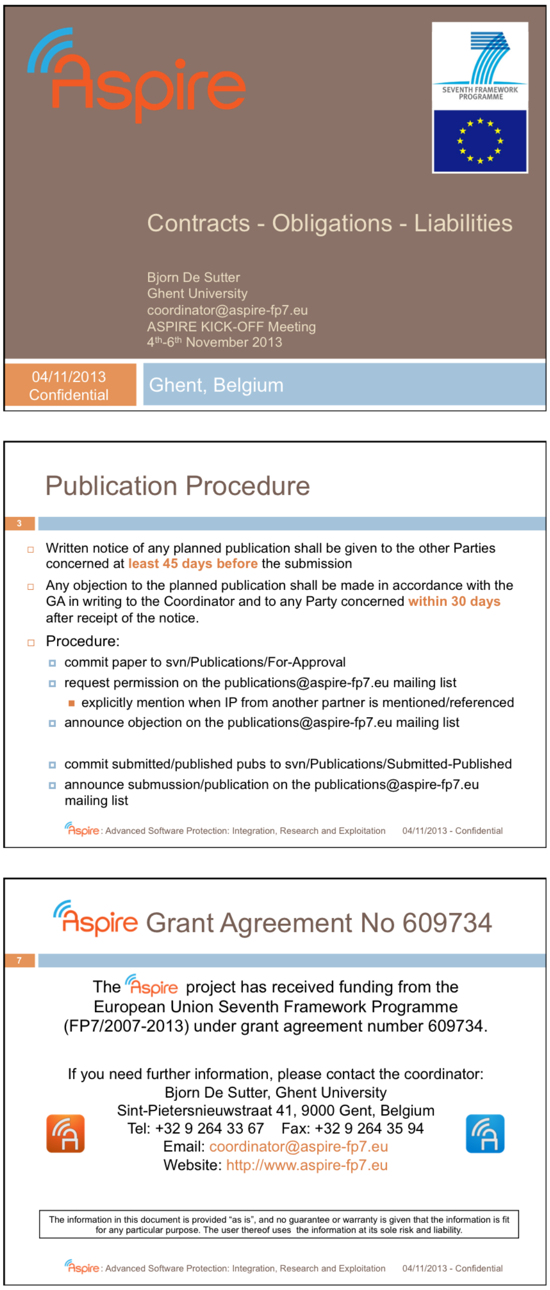


Figure 2 - ASPIRE buttons

1.2 Templates

In order to streamline the dissemination of ASPIRE results and create a recognition of ASPIRE graphical material in the software protection community, a Word template was created (of which the use of this report shows what it looks like), and a similar looking LaTeX style was also created along with a PowerPoint presentation template: some example slides are depicted in Figure 3.



SEVENTH FRAMEWORK PROGRAMME

Contracts - Obligations - Liabilities

Bjorn De Sutter
Ghent University
coordinator@aspire-fp7.eu
ASPIRE KICK-OFF Meeting
4th-6th November 2013

04/11/2013
Confidential

Ghent, Belgium

Publication Procedure

3

- Written notice of any planned publication shall be given to the other Parties concerned at **least 45 days before** the submission
- Any objection to the planned publication shall be made in accordance with the GA in writing to the Coordinator and to any Party concerned **within 30 days** after receipt of the notice.
- Procedure:
  - commit paper to svn/Publications/For-Approval
  - request permission on the publications@aspire-fp7.eu mailing list
    - explicitly mention when IP from another partner is mentioned/referenced
  - announce objection on the publications@aspire-fp7.eu mailing list
  - commit submitted/published pubs to svn/Publications/Submitted-Published
  - announce submussion/publication on the publications@aspire-fp7.eu mailing list

Aspire : Advanced Software Protection: Integration, Research and Exploitation 04/11/2013 - Confidential

Aspire Grant Agreement No 609734

7

The Aspire project has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement number 609734.

If you need further information, please contact the coordinator:
Bjorn De Sutter, Ghent University
Sint-Pietersnieuwstraat 41, 9000 Gent, Belgium
Tel: +32 9 264 33 67 Fax: +32 9 264 35 94
Email: coordinator@aspire-fp7.eu
Website: http://www.aspire-fp7.eu

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

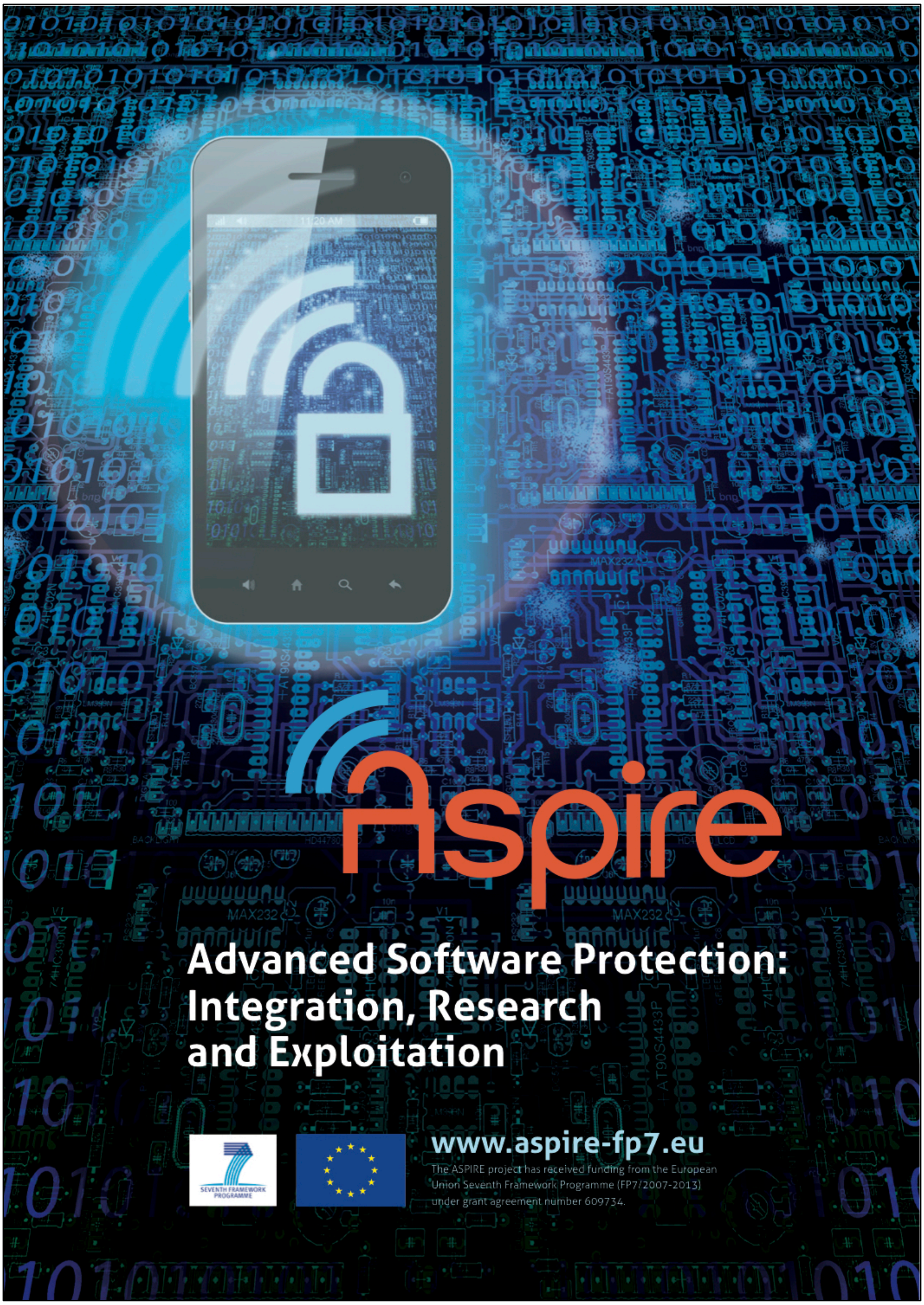
Aspire : Advanced Software Protection: Integration, Research and Exploitation 04/11/2013 - Confidential

Figure 3 - Examples of ASPIRE presentation template

1.3 Project Leaflet

As soon as the project had started, the communication company Magelaan (www.Magelaan.be) was hired to design a project leaflet that can be handed out by the project partners at networking events. Reduced quality versions of this 4-page A4 leaflet are shown in Figure 4 to Figure 7.

This flyer was distributed at multiple local and international events by multiple project partners.

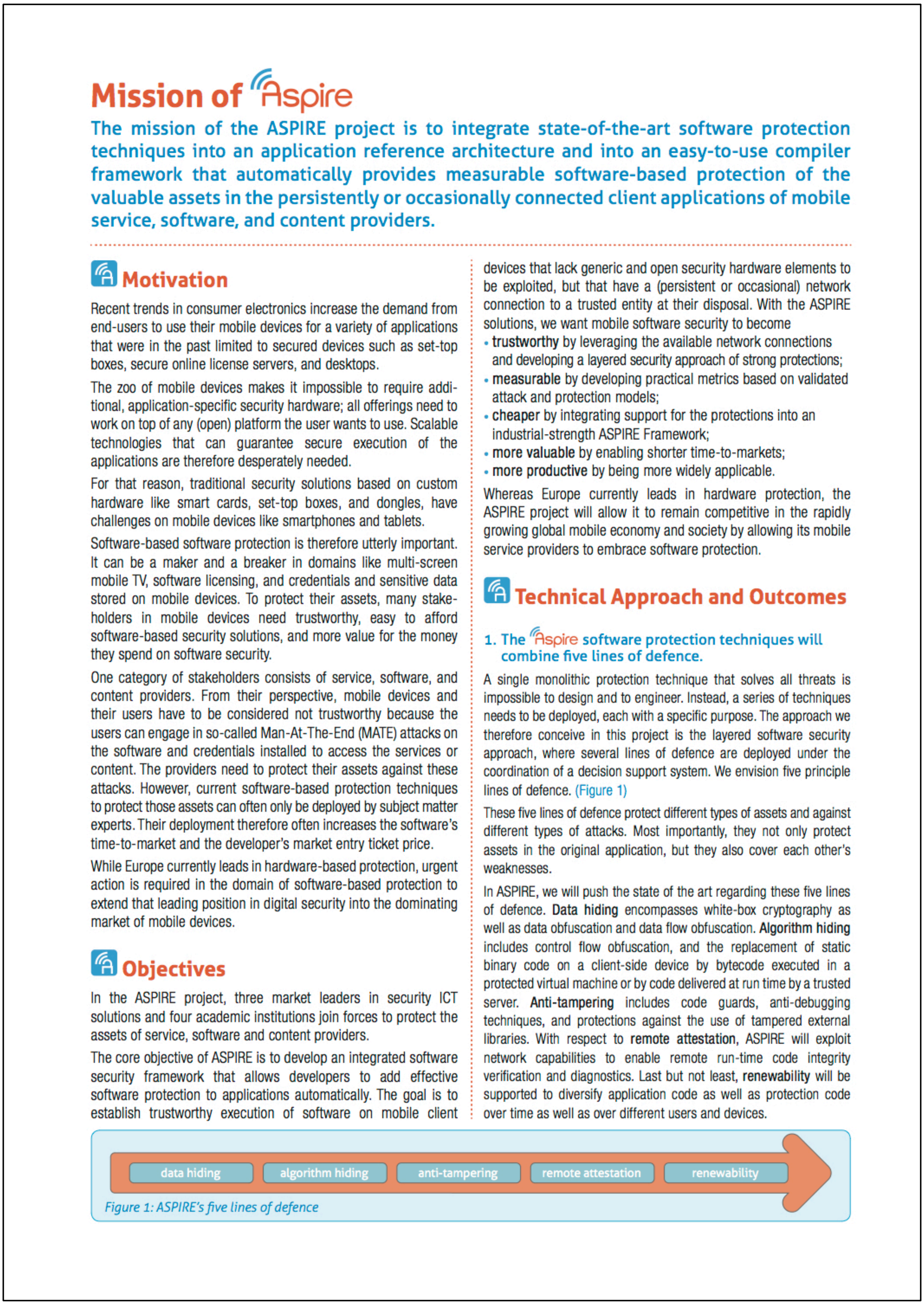


Advanced Software Protection: Integration, Research and Exploitation

www.aspire-fp7.eu

The ASPIRE project has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement number 609734.

Figure 4 - Front page ASPIRE leaflet



Mission of Aspire

The mission of the ASPIRE project is to integrate state-of-the-art software protection techniques into an application reference architecture and into an easy-to-use compiler framework that automatically provides measurable software-based protection of the valuable assets in the persistently or occasionally connected client applications of mobile service, software, and content providers.

Motivation

Recent trends in consumer electronics increase the demand from end-users to use their mobile devices for a variety of applications that were in the past limited to secured devices such as set-top boxes, secure online license servers, and desktops.

The zoo of mobile devices makes it impossible to require additional, application-specific security hardware; all offerings need to work on top of any (open) platform the user wants to use. Scalable technologies that can guarantee secure execution of the applications are therefore desperately needed.

For that reason, traditional security solutions based on custom hardware like smart cards, set-top boxes, and dongles, have challenges on mobile devices like smartphones and tablets.

Software-based software protection is therefore utterly important. It can be a maker and a breaker in domains like multi-screen mobile TV, software licensing, and credentials and sensitive data stored on mobile devices. To protect their assets, many stakeholders in mobile devices need trustworthy, easy to afford software-based security solutions, and more value for the money they spend on software security.

One category of stakeholders consists of service, software, and content providers. From their perspective, mobile devices and their users have to be considered not trustworthy because the users can engage in so-called Man-At-The-End (MATE) attacks on the software and credentials installed to access the services or content. The providers need to protect their assets against these attacks. However, current software-based protection techniques to protect those assets can often only be deployed by subject matter experts. Their deployment therefore often increases the software's time-to-market and the developer's market entry ticket price.

While Europe currently leads in hardware-based protection, urgent action is required in the domain of software-based protection to extend that leading position in digital security into the dominating market of mobile devices.

Objectives

In the ASPIRE project, three market leaders in security ICT solutions and four academic institutions join forces to protect the assets of service, software and content providers.

The core objective of ASPIRE is to develop an integrated software security framework that allows developers to add effective software protection to applications automatically. The goal is to establish trustworthy execution of software on mobile client devices that lack generic and open security hardware elements to be exploited, but that have a (persistent or occasional) network connection to a trusted entity at their disposal. With the ASPIRE solutions, we want mobile software security to become

- **trustworthy** by leveraging the available network connections and developing a layered security approach of strong protections;
- **measurable** by developing practical metrics based on validated attack and protection models;
- **cheaper** by integrating support for the protections into an industrial-strength ASPIRE Framework;
- **more valuable** by enabling shorter time-to-markets;
- **more productive** by being more widely applicable.

Whereas Europe currently leads in hardware protection, the ASPIRE project will allow it to remain competitive in the rapidly growing global mobile economy and society by allowing its mobile service providers to embrace software protection.

Technical Approach and Outcomes

1. The Aspire software protection techniques will combine five lines of defence.

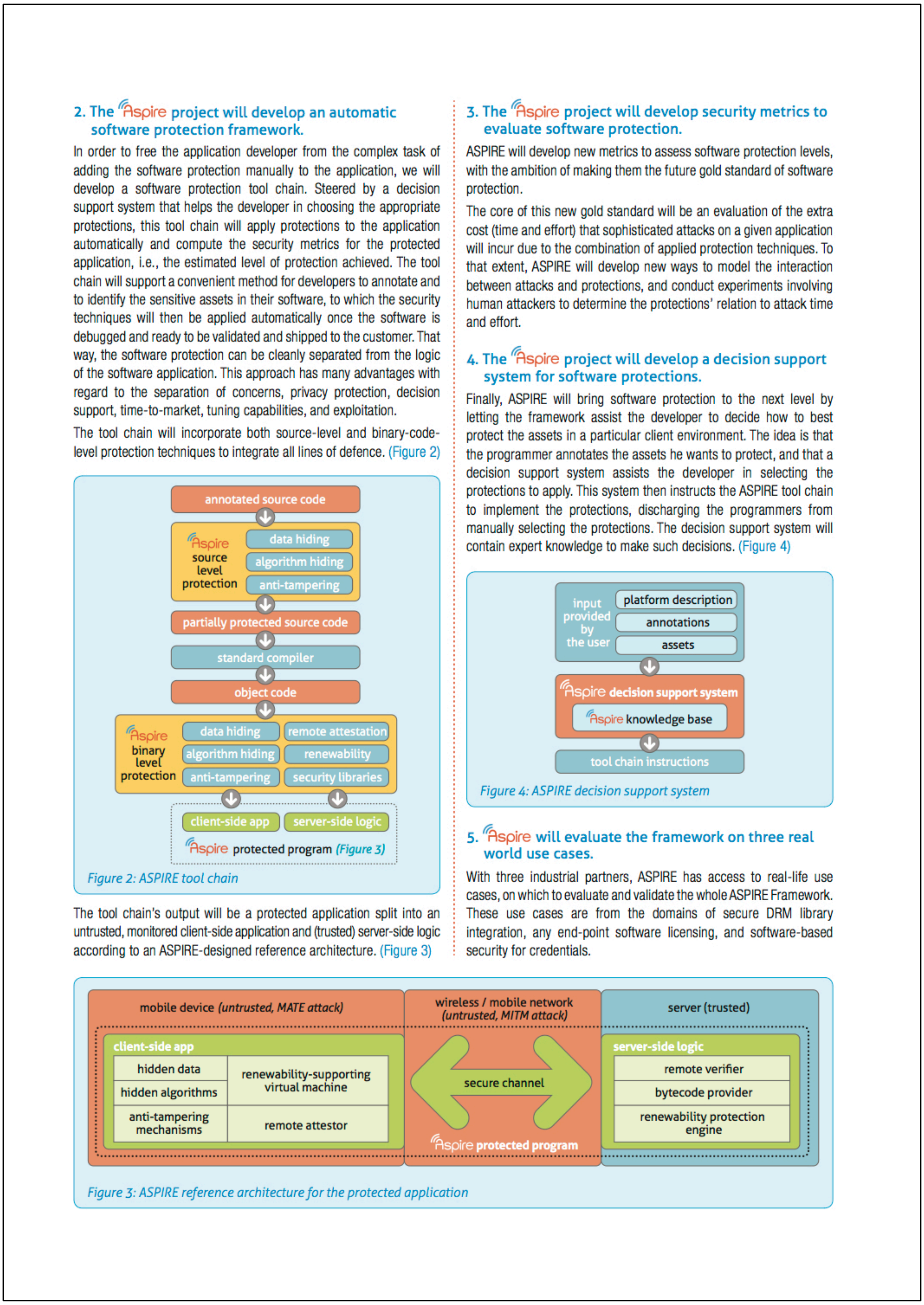
A single monolithic protection technique that solves all threats is impossible to design and to engineer. Instead, a series of techniques needs to be deployed, each with a specific purpose. The approach we therefore conceive in this project is the layered software security approach, where several lines of defence are deployed under the coordination of a decision support system. We envision five principle lines of defence. (Figure 1)

These five lines of defence protect different types of assets and against different types of attacks. Most importantly, they not only protect assets in the original application, but they also cover each other's weaknesses.

In ASPIRE, we will push the state of the art regarding these five lines of defence. **Data hiding** encompasses white-box cryptography as well as data obfuscation and data flow obfuscation. **Algorithm hiding** includes control flow obfuscation, and the replacement of static binary code on a client-side device by bytecode executed in a protected virtual machine or by code delivered at run time by a trusted server. **Anti-tampering** includes code guards, anti-debugging techniques, and protections against the use of tampered external libraries. With respect to **remote attestation**, ASPIRE will exploit network capabilities to enable remote run-time code integrity verification and diagnostics. Last but not least, **renewability** will be supported to diversify application code as well as protection code over time as well as over different users and devices.

Figure 1: ASPIRE's five lines of defence

Figure 5 - Page 2 ASPIRE leaflet



2. The Aspire project will develop an automatic software protection framework.

In order to free the application developer from the complex task of adding the software protection manually to the application, we will develop a software protection tool chain. Steered by a decision support system that helps the developer in choosing the appropriate protections, this tool chain will apply protections to the application automatically and compute the security metrics for the protected application, i.e., the estimated level of protection achieved. The tool chain will support a convenient method for developers to annotate and to identify the sensitive assets in their software, to which the security techniques will then be applied automatically once the software is debugged and ready to be validated and shipped to the customer. That way, the software protection can be cleanly separated from the logic of the software application. This approach has many advantages with regard to the separation of concerns, privacy protection, decision support, time-to-market, tuning capabilities, and exploitation.

The tool chain will incorporate both source-level and binary-code-level protection techniques to integrate all lines of defence. (Figure 2)

Figure 2: ASPIRE tool chain

The tool chain's output will be a protected application split into an untrusted, monitored client-side application and (trusted) server-side logic according to an ASPIRE-designed reference architecture. (Figure 3)

3. The Aspire project will develop security metrics to evaluate software protection.

ASPIRE will develop new metrics to assess software protection levels, with the ambition of making them the future gold standard of software protection.

The core of this new gold standard will be an evaluation of the extra cost (time and effort) that sophisticated attacks on a given application will incur due to the combination of applied protection techniques. To that extent, ASPIRE will develop new ways to model the interaction between attacks and protections, and conduct experiments involving human attackers to determine the protections' relation to attack time and effort.

4. The Aspire project will develop a decision support system for software protections.

Finally, ASPIRE will bring software protection to the next level by letting the framework assist the developer to decide how to best protect the assets in a particular client environment. The idea is that the programmer annotates the assets he wants to protect, and that a decision support system assists the developer in selecting the protections to apply. This system then instructs the ASPIRE tool chain to implement the protections, discharging the programmers from manually selecting the protections. The decision support system will contain expert knowledge to make such decisions. (Figure 4)

Figure 4: ASPIRE decision support system

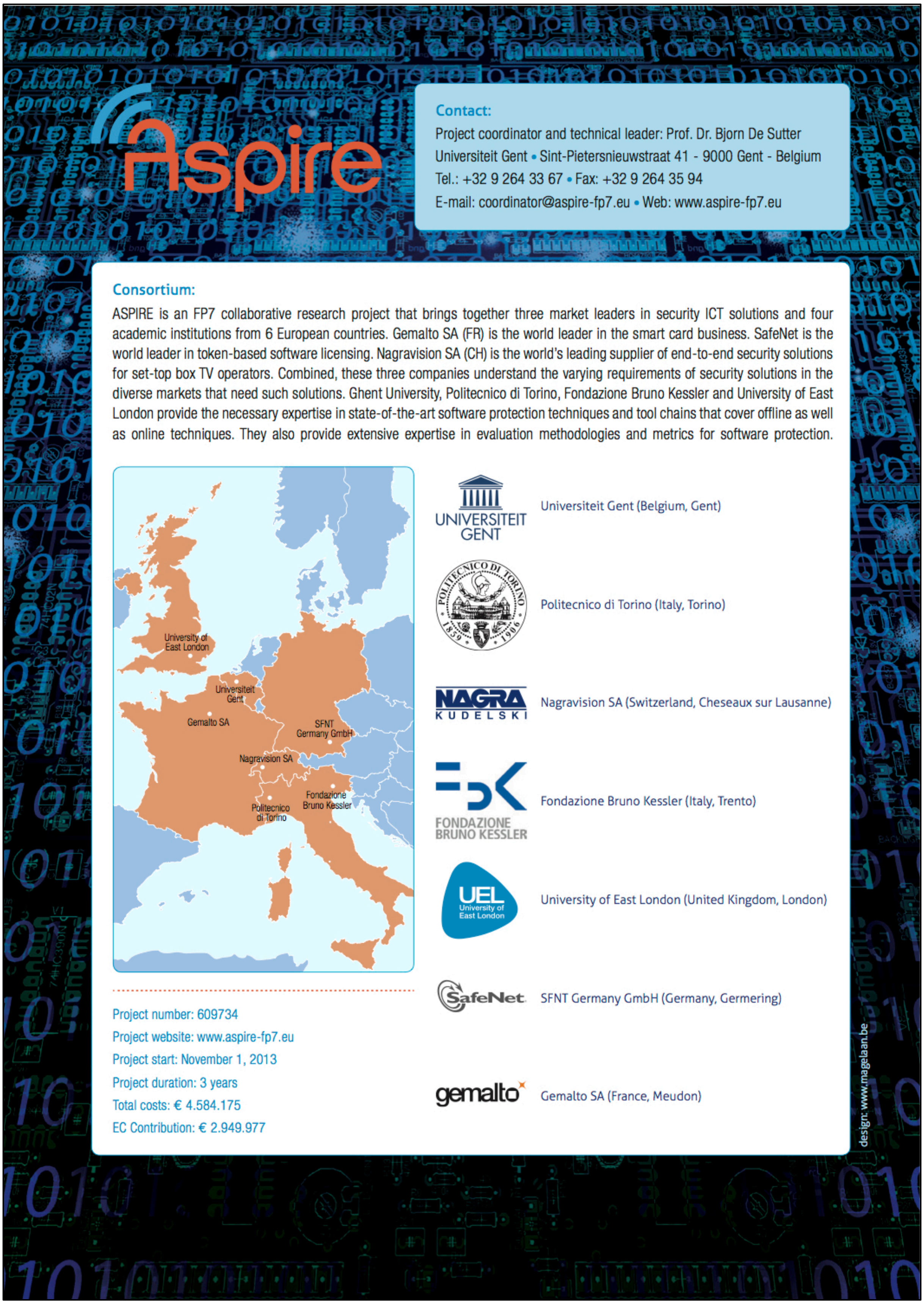
5. Aspire will evaluate the framework on three real world use cases.

With three industrial partners, ASPIRE has access to real-life use cases, on which to evaluate and validate the whole ASPIRE Framework. These use cases are from the domains of secure DRM library integration, any end-point software licensing, and software-based security for credentials.

mobile device (untrusted, MATE attack)
wireless / mobile network (untrusted, MITM attack)
server (trusted)
client-side app
hidden data
hidden algorithms
anti-tampering mechanisms
renewability-supporting virtual machine
remote attestor
secure channel
Aspire protected program
server-side logic
remote verifier
bytecode provider
renewability protection engine

Figure 3: ASPIRE reference architecture for the protected application

Figure 6 - Page 3 ASPIRE leaflet



Contact:

Project coordinator and technical leader: Prof. Dr. Bjorn De Sutter
Universiteit Gent • Sint-Pietersnieuwstraat 41 - 9000 Gent - Belgium
Tel.: +32 9 264 33 67 • Fax: +32 9 264 35 94
E-mail: coordinator@aspire-fp7.eu • Web: www.aspire-fp7.eu

Consortium:

ASPIRE is an FP7 collaborative research project that brings together three market leaders in security ICT solutions and four academic institutions from 6 European countries. Gemalto SA (FR) is the world leader in the smart card business. SafeNet is the world leader in token-based software licensing. Nagravision SA (CH) is the world's leading supplier of end-to-end security solutions for set-top box TV operators. Combined, these three companies understand the varying requirements of security solutions in the diverse markets that need such solutions. Ghent University, Politecnico di Torino, Fondazione Bruno Kessler and University of East London provide the necessary expertise in state-of-the-art software protection techniques and tool chains that cover offline as well as online techniques. They also provide extensive expertise in evaluation methodologies and metrics for software protection.

Universiteit Gent (Belgium, Gent)

Politecnico di Torino (Italy, Torino)

Nagravision SA (Switzerland, Cheseaux sur Lausanne)

Fondazione Bruno Kessler (Italy, Trento)

University of East London (United Kingdom, London)

SFNT Germany GmbH (Germany, Germering)

Gemalto SA (France, Meudon)

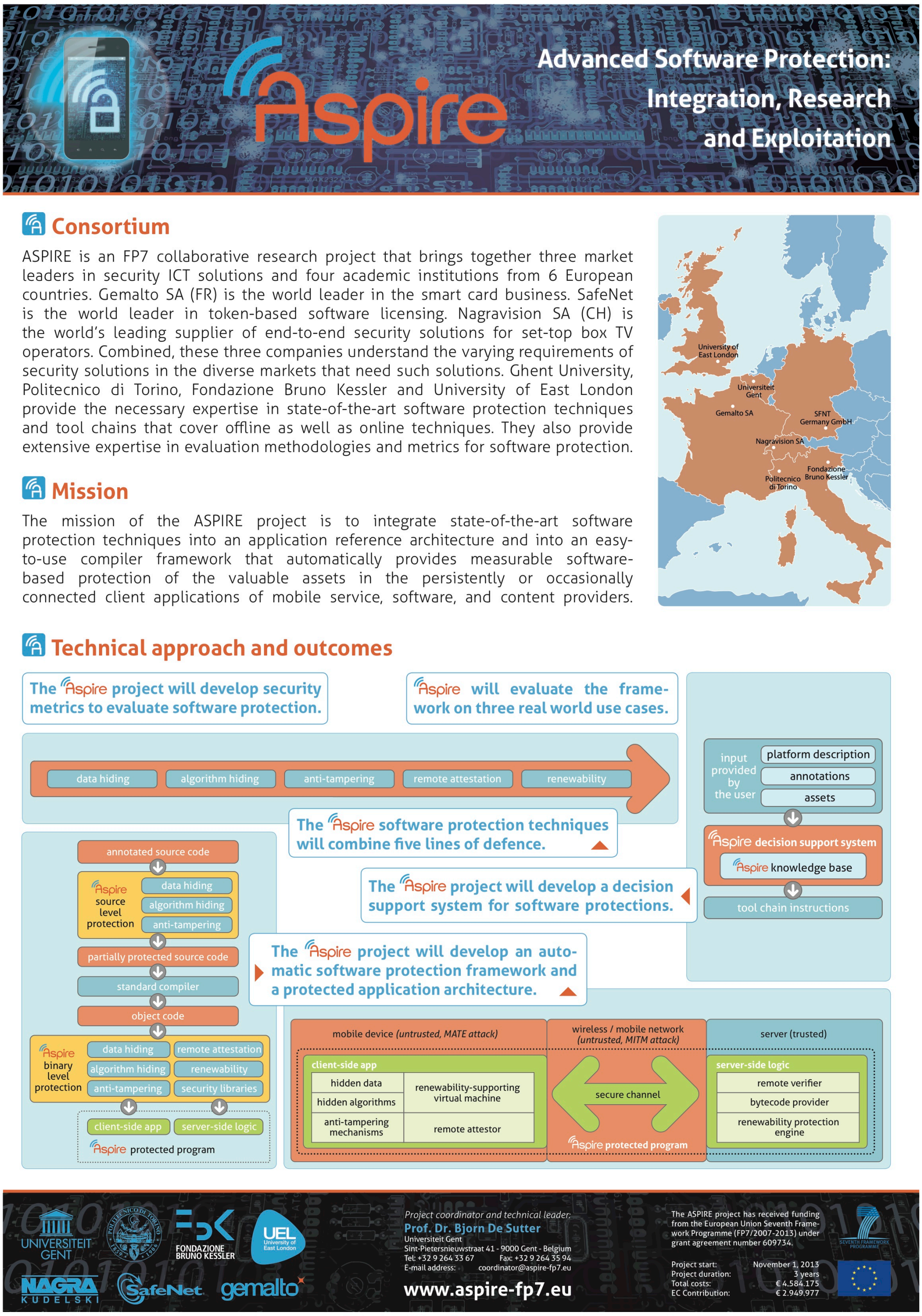
Project number: 609734
Project website: www.aspire-fp7.eu
Project start: November 1, 2013
Project duration: 3 years
Total costs: € 4.584.175
EC Contribution: € 2.949.977

design: www.magelaan.be

Figure 7 - Back page ASPIRE leaflet

1.4 Project Poster

On the basis of the project leaflet graphics, we also designed (internally) a general ASPIRE poster that can be reused by all partners at poster events. This A0-poster is depicted in Figure 8 at reduced resolution.



Aspire

Advanced Software Protection:
Integration, Research
and Exploitation

Consortium

ASPIRE is an FP7 collaborative research project that brings together three market leaders in security ICT solutions and four academic institutions from 6 European countries. Gemalto SA (FR) is the world leader in the smart card business. SafeNet is the world leader in token-based software licensing. Nagravision SA (CH) is the world's leading supplier of end-to-end security solutions for set-top box TV operators. Combined, these three companies understand the varying requirements of security solutions in the diverse markets that need such solutions. Ghent University, Politecnico di Torino, Fondazione Bruno Kessler and University of East London provide the necessary expertise in state-of-the-art software protection techniques and tool chains that cover offline as well as online techniques. They also provide extensive expertise in evaluation methodologies and metrics for software protection.

Mission

The mission of the ASPIRE project is to integrate state-of-the-art software protection techniques into an application reference architecture and into an easy-to-use compiler framework that automatically provides measurable software-based protection of the valuable assets in the persistently or occasionally connected client applications of mobile service, software, and content providers.

Technical approach and outcomes

The Aspire project will develop security metrics to evaluate software protection.

Aspire will evaluate the framework on three real world use cases.

The Aspire software protection techniques will combine five lines of defence.

The Aspire project will develop a decision support system for software protections.

The Aspire project will develop an automatic software protection framework and a protected application architecture.

Project coordinator and technical leader:
Prof. Dr. Bjorn De Sutter
Universiteit Gent
Sint-Pietersnieuwstraat 41 - 9000 Gent - Belgium
Tel: +32 9 264 33 67 Fax: +32 9 264 35 94
E-mail address: coordinator@aspire-fp7.eu

www.aspire-fp7.eu

The ASPIRE project has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement number 609734.

Project start:	November 1, 2013
Project duration:	3 years
Total costs:	€ 4.584.175
EC Contribution:	€ 2.949.977

Figure 8 - ASPIRE poster

Section 2 Online Presence

Chapter Authors: Bjorn De Sutter (UGent), Elena Gómez-Martínez (UEL)

2.1 ASPIRE Project Website

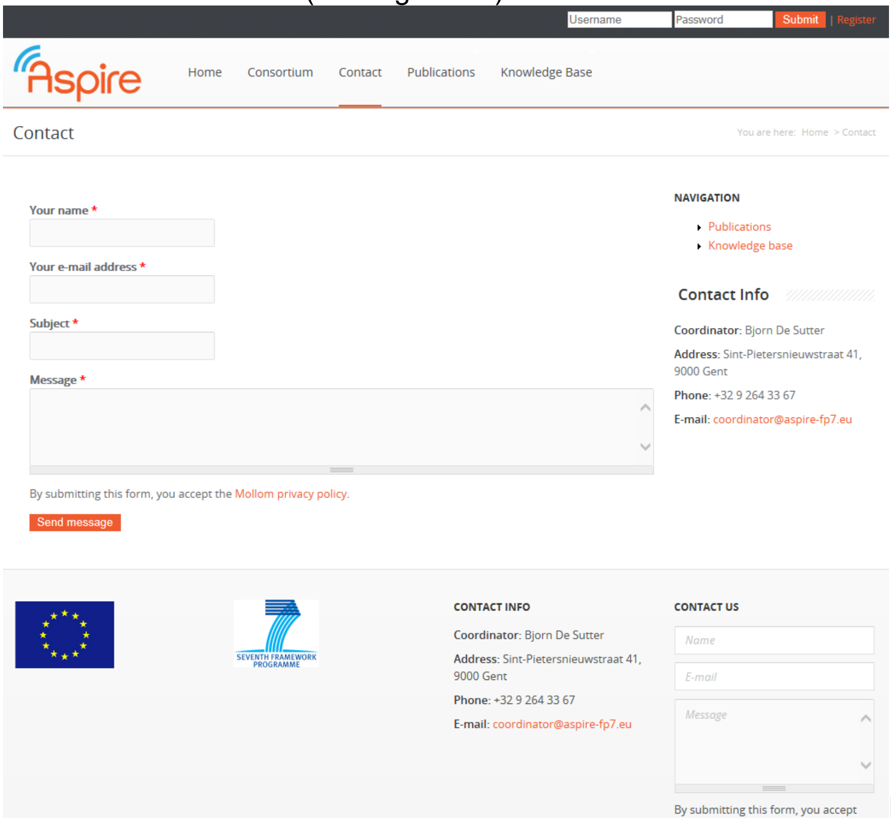
2.1.1 Public ASPIRE Website https://www.aspire-fp7.eu

To serve the broadest possible visibility of the project, the project website was launched in the first month of the project. The website builds on the Drupal Content Management System (https://drupal.org/). All pages on this public website are available to everyone, it is not necessary to login.

The website can be accessed with all major browsers, and a Drupal Theme was licensed and utilized to automatically adapt and reformat the page layout for the screen sizes and resolutions used on several types of Internet access points, ranging from small, touchscreen smart phones, over larger screen tablets, to laptops and desktop computers.

The website will be maintained for three years after the end of the project. Currently, the public part of the website consists of the following pages:

- **Home**: General introduction to the project, brief overview of consortium by means of partner logos. See Figure 9 for screenshot of the home page on a desktop browser. Figure 10 shows a screenshot on the iOS smartphone browser as demonstration of the portability of the used theme.
- **Consortium**: Description of all project partners and principal investigators (see Figure 11).
- **Contact**: Contact form (see Figure 12).



By submitting this form, you accept the Mollom privacy policy.

Coordinator: Bjorn De Sutter
Address: Sint-Pietersnieuwstraat 41, 9000 Gent
Phone: +32 9 264 33 67
E-mail: coordinator@aspire-fp7.eu

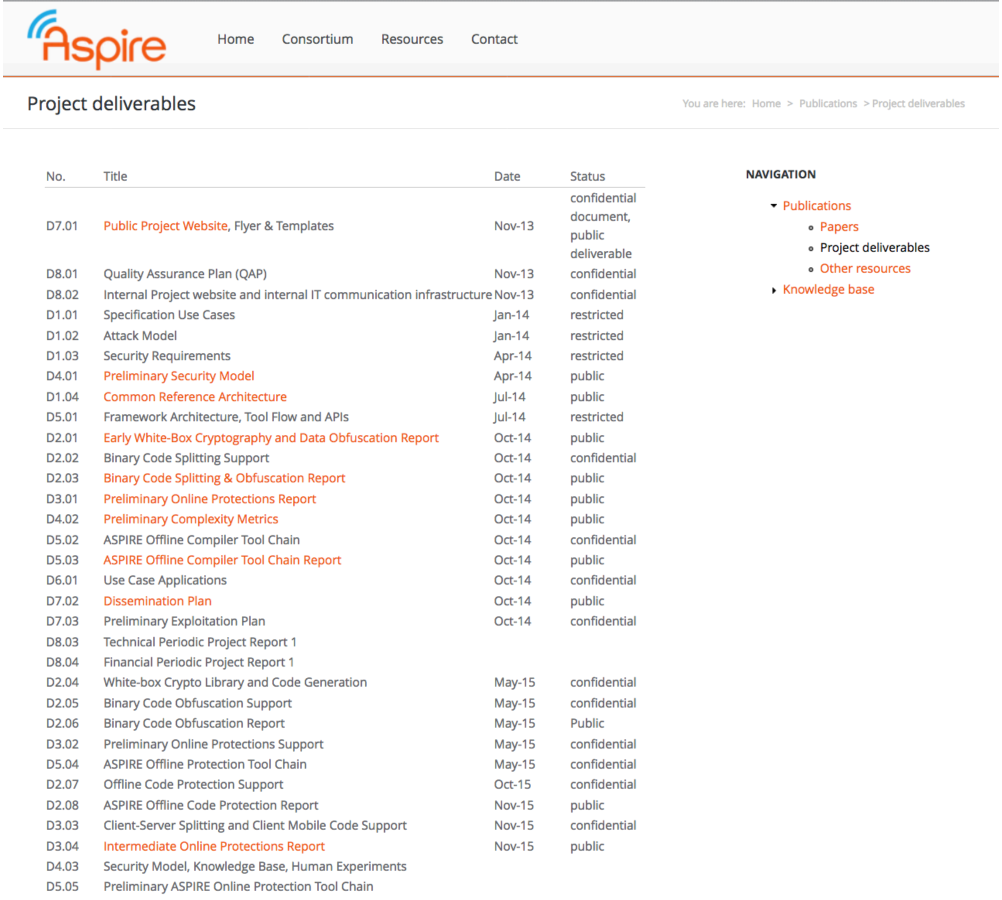
Coordinator: Bjorn De Sutter
Address: Sint-Pietersnieuwstraat 41, 9000 Gent
Phone: +32 9 264 33 67
E-mail: coordinator@aspire-fp7.eu

By submitting this form, you accept

- **Resources:** container of all public resources:
  - **ASPIRE papers**: It includes published papers, all public project deliverables, which have been accepted and other resource, such as videos. Publications can be

selected and ranked based on subject (metrics, obfuscations, program analyses, etc…) and year (see Figure 13).

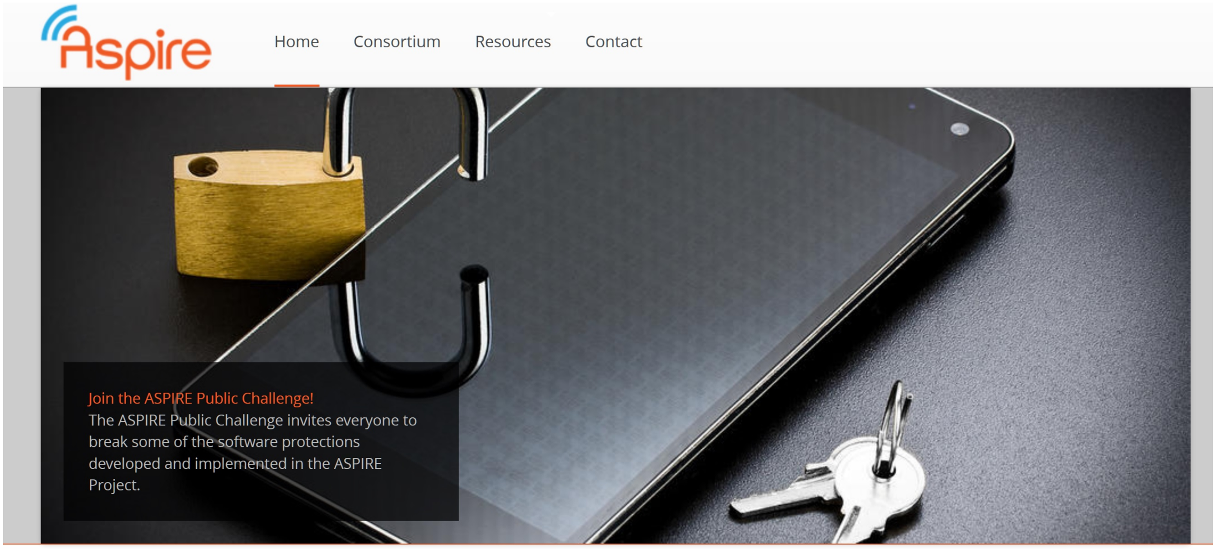
- **Knowledge base:** It includes published papers too and related sites interesting for the project. Publications can be selected and ranked based on subject (metrics, obfuscations, program analyses, etc.) and year (see Figure 14).
- **Project Deliverables:** It includes a list of ASPIRE project deliverables (see Figure 15).



Project deliverables

No.	Title	Date	Status
D7.01	Public Project Website, Flyer & Templates	Nov-13	confidential document, public deliverable
D8.01	Quality Assurance Plan (QAP)	Nov-13	confidential
D8.02	Internal Project website and internal IT communication infrastructure	Nov-13	confidential
D1.01	Specification Use Cases	Jan-14	restricted
D1.02	Attack Model	Jan-14	restricted
D1.03	Security Requirements	Apr-14	restricted
D4.01	Preliminary Security Model	Apr-14	public
D1.04	Common Reference Architecture	Jul-14	public
D5.01	Framework Architecture, Tool Flow and APIs	Jul-14	restricted
D2.01	Early White-Box Cryptography and Data Obfuscation Report	Oct-14	public
D2.02	Binary Code Splitting Support	Oct-14	confidential
D2.03	Binary Code Splitting & Obfuscation Report	Oct-14	public
D3.01	Preliminary Online Protections Report	Oct-14	public
D4.02	Preliminary Complexity Metrics	Oct-14	public
D5.02	ASPIRE Offline Compiler Tool Chain	Oct-14	confidential
D5.03	ASPIRE Offline Compiler Tool Chain Report	Oct-14	public
D6.01	Use Case Applications	Oct-14	confidential
D7.02	Dissemination Plan	Oct-14	public
D7.03	Preliminary Exploitation Plan	Oct-14	confidential
D8.03	Technical Periodic Project Report 1		
D8.04	Financial Periodic Project Report 1		
D2.04	White-box Crypto Library and Code Generation	May-15	confidential
D2.05	Binary Code Obfuscation Support	May-15	confidential
D2.06	Binary Code Obfuscation Report	May-15	Public
D3.02	Preliminary Online Protections Support	May-15	confidential
D5.04	ASPIRE Offline Protection Tool Chain	May-15	confidential
D2.07	Offline Code Protection Support	Oct-15	confidential
D2.08	ASPIRE Offline Code Protection Report	Nov-15	public
D3.03	Client-Server Splitting and Client Mobile Code Support	Nov-15	confidential
D3.04	Intermediate Online Protections Report	Nov-15	public
D4.03	Security Model, Knowledge Base, Human Experiments		
D5.05	Preliminary ASPIRE Online Protection Tool Chain		

- **Source code:** contains the link to the github repositories in which most of the ASPIRE code has been published with open-source licenses;
- **Demo Videos**: contains the link to the ASPIRE YouTube channel with all the videos on different project results;
- **Other Resources**: contains various resources, such as a TV interview, project leaflets, keynote talks, invited lectures, and press-releases.

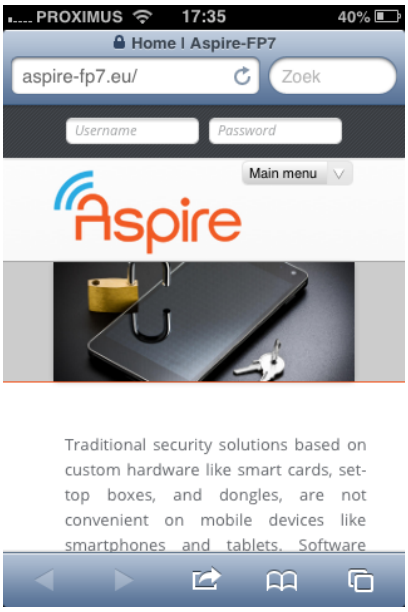


Join the ASPIRE Public Challenge!
The ASPIRE Public Challenge invites everyone to break some of the software protections developed and implemented in the ASPIRE Project.

Traditional security solutions based on custom hardware like smart cards, set-top boxes, and dongles, are not convenient on mobile devices like smartphones and tablets. Software protection is therefore utterly important; it can be a maker and a breaker in domains like multi-screen mobile TV, software licensing, and credentials and sensitive data stored on mobile devices. However, current software protection techniques are incredibly hard to deploy. Moreover, they cost too much and limit innovation. Therefore many stakeholders in mobile devices need more trustworthy, cheaper software security solutions and more value for the money they spend on security.

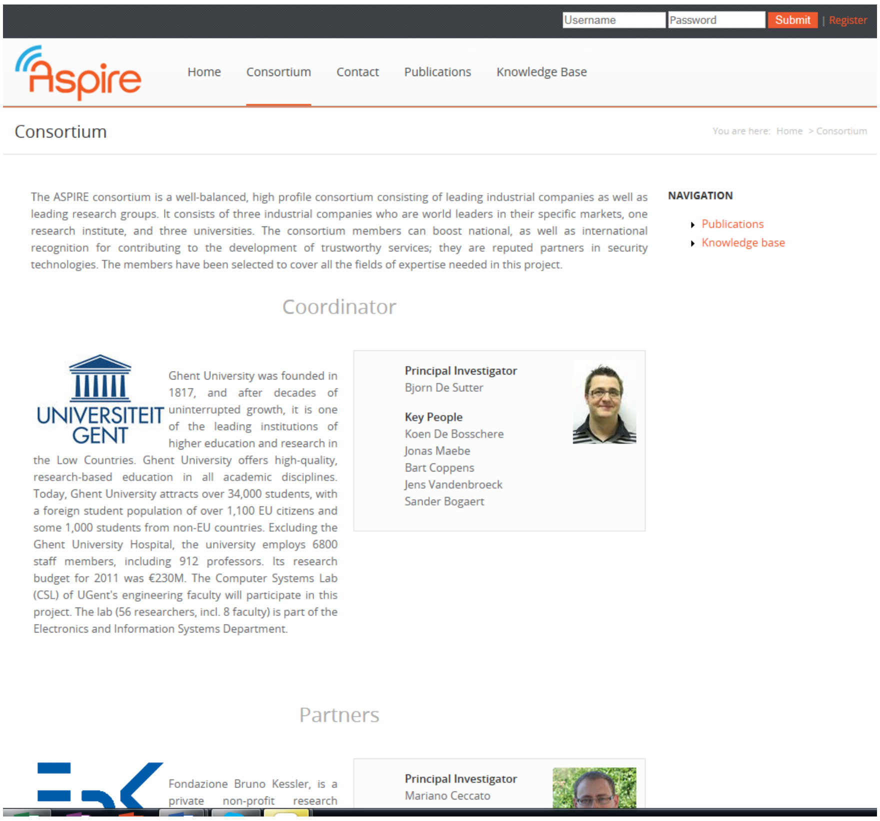
In this project, three market leaders in security ICT solutions and four academic institutions join forces to protect the

Figure 9 - Screenshot of the top part of the home page on the ASPIRE website



Traditional security solutions based on custom hardware like smart cards, set-top boxes, and dongles, are not convenient on mobile devices like smartphones and tablets. Software

Figure 10 - Screenshot of the ASPIRE website home page on an iPhone 3G.



Consortium

You are here: Home > Consortium

The ASPIRE consortium is a well-balanced, high profile consortium consisting of leading industrial companies as well as leading research groups. It consists of three industrial companies who are world leaders in their specific markets, one research institute, and three universities. The consortium members can boost national, as well as international recognition for contributing to the development of trustworthy services; they are reputed partners in security technologies. The members have been selected to cover all the fields of expertise needed in this project.

NAVIGATION

- Publications
- Knowledge base

Coordinator

UNIVERSITEIT GENT

Ghent University was founded in 1817, and after decades of uninterrupted growth, it is one of the leading institutions of higher education and research in the Low Countries. Ghent University offers high-quality, research-based education in all academic disciplines. Today, Ghent University attracts over 34,000 students, with a foreign student population of over 1,100 EU citizens and some 1,000 students from non-EU countries. Excluding the Ghent University Hospital, the university employs 6800 staff members, including 912 professors. Its research budget for 2011 was €230M. The Computer Systems Lab (CSL) of UGent's engineering faculty will participate in this project. The lab (56 researchers, incl. 8 faculty) is part of the Electronics and Information Systems Department.

Principal Investigator
Bjorn De Sutter

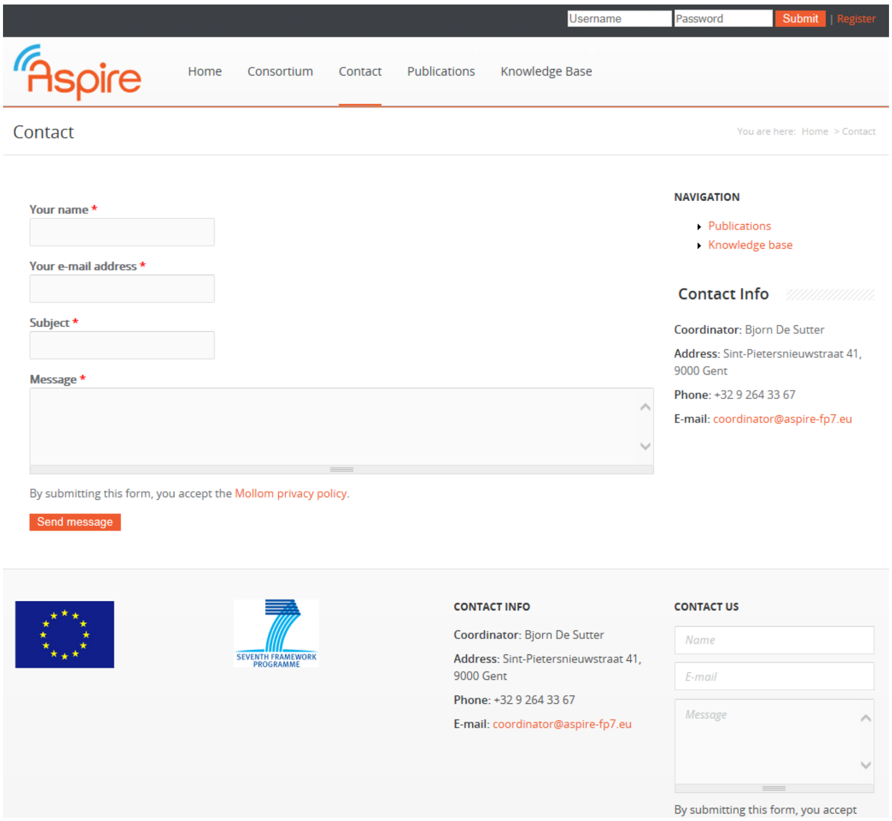
Key People
Koen De Bosschere
Jonas Maebe
Bart Coppens
Jens Vandenbroeck
Sander Bogaert

Partners

Fondazione Bruno Kessler, is a private non-profit research

Principal Investigator
Mariano Ceccato

Figure 11 - Screenshot of the consortium page on the ASPIRE website



Contact

You are here: Home > Contact

Your name *

Your e-mail address *

Subject *

Message *

By submitting this form, you accept the Mollom privacy policy.

NAVIGATION

- Publications
- Knowledge base

Contact Info

Coordinator: Bjorn De Sutter

Address: Sint-Pietersnieuwstraat 41, 9000 Gent

Phone: +32 9 264 33 67

E-mail: coordinator@aspire-fp7.eu

CONTACT INFO

Coordinator: Bjorn De Sutter

Address: Sint-Pietersnieuwstraat 41, 9000 Gent

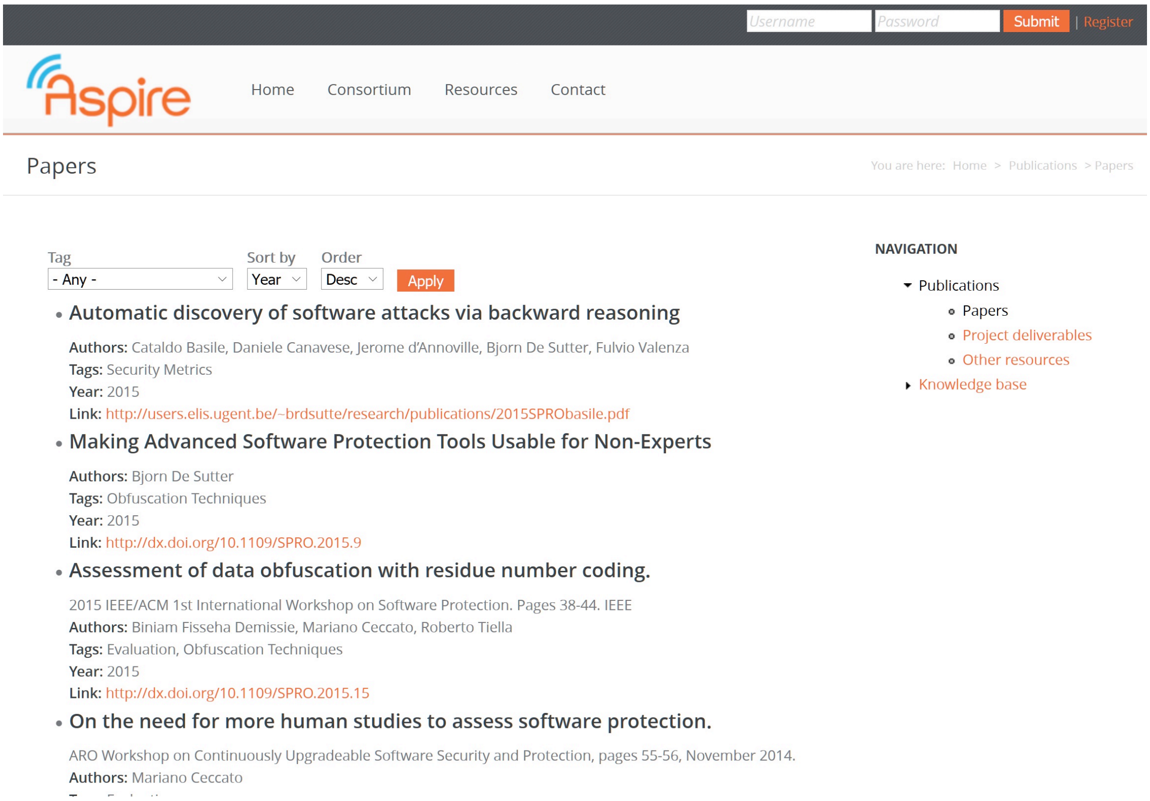
Phone: +32 9 264 33 67

E-mail: coordinator@aspire-fp7.eu

CONTACT US

By submitting this form, you accept

Figure 12 - Screenshot of the contact form on the ASPIRE website



Papers

- Automatic discovery of software attacks via backward reasoning

  Authors: Cataldo Basile, Daniele Canavese, Jerome d'Annoville, Bjorn De Sutter, Fulvio Valenza
  Tags: Security Metrics
  Year: 2015
  Link: http://users.elis.ugent.be/~brdsutte/research/publications/2015SPRObasile.pdf

- Making Advanced Software Protection Tools Usable for Non-Experts

  Authors: Bjorn De Sutter
  Tags: Obfuscation Techniques
  Year: 2015
  Link: http://dx.doi.org/10.1109/SPRO.2015.9

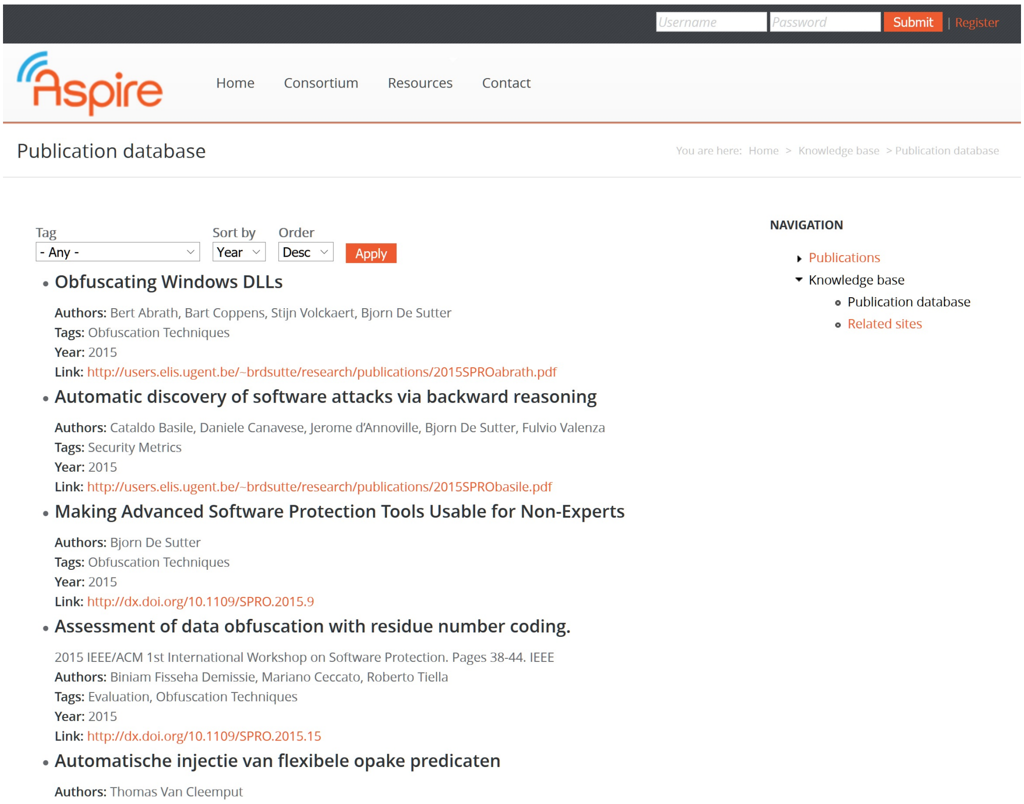
- Assessment of data obfuscation with residue number coding.

  2015 IEEE/ACM 1st International Workshop on Software Protection. Pages 38-44. IEEE
  Authors: Biniam Fisseha Demissie, Mariano Ceccato, Roberto Tiella
  Tags: Evaluation, Obfuscation Techniques
  Year: 2015
  Link: http://dx.doi.org/10.1109/SPRO.2015.15

- On the need for more human studies to assess software protection.

  ARO Workshop on Continuously Upgradeable Software Security and Protection, pages 55-56, November 2014.
  Authors: Mariano Ceccato

Figure 13- Screenshot of the publications page on the ASPIRE website



Publication database

- Obfuscating Windows DLLs

  Authors: Bert Abrath, Bart Coppens, Stijn Volckaert, Bjorn De Sutter
  Tags: Obfuscation Techniques
  Year: 2015
  Link: http://users.elis.ugent.be/~brdsutte/research/publications/2015SPROabrath.pdf

- Automatic discovery of software attacks via backward reasoning

  Authors: Cataldo Basile, Daniele Canavese, Jerome d'Annoville, Bjorn De Sutter, Fulvio Valenza
  Tags: Security Metrics
  Year: 2015
  Link: http://users.elis.ugent.be/~brdsutte/research/publications/2015SPRObasile.pdf

- Making Advanced Software Protection Tools Usable for Non-Experts

  Authors: Bjorn De Sutter
  Tags: Obfuscation Techniques
  Year: 2015
  Link: http://dx.doi.org/10.1109/SPRO.2015.9

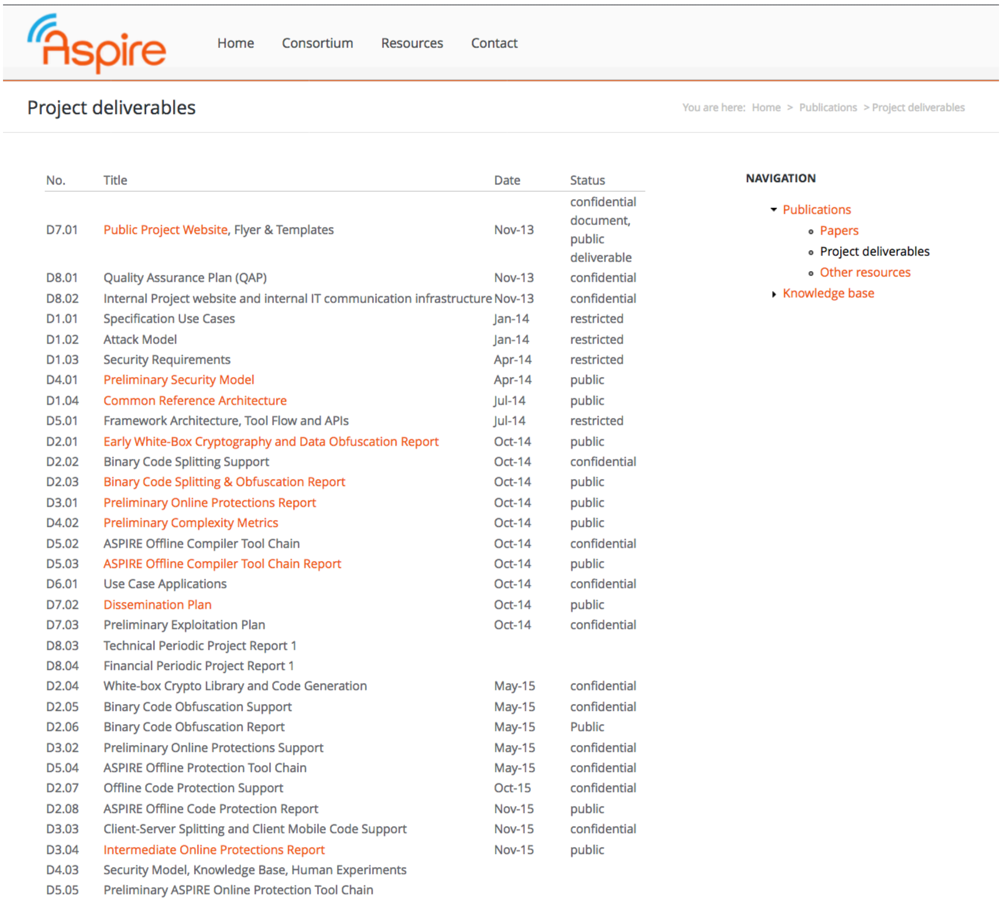
- Assessment of data obfuscation with residue number coding.

  2015 IEEE/ACM 1st International Workshop on Software Protection. Pages 38-44. IEEE
  Authors: Biniam Fisseha Demissie, Mariano Ceccato, Roberto Tiella
  Tags: Evaluation, Obfuscation Techniques
  Year: 2015
  Link: http://dx.doi.org/10.1109/SPRO.2015.15

- Automatische injectie van flexibele opake predicaten

  Authors: Thomas Van Cleemput

Figure 14- Screenshot of knowledge base page on the ASPIRE website



Project deliverables

You are here: Home > Publications > Project deliverables

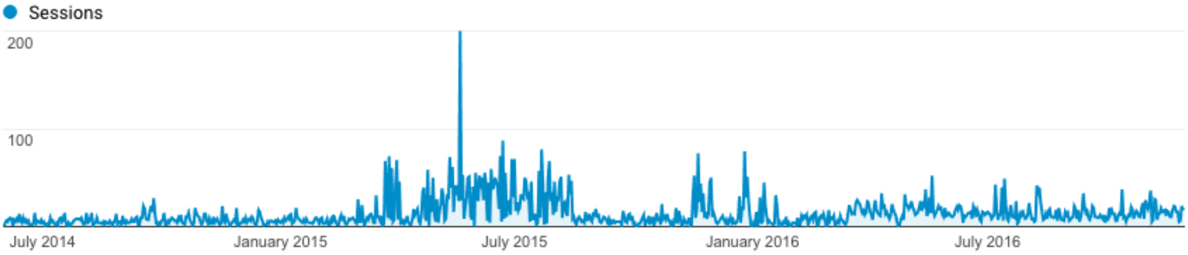
No.	Title	Date	Status
D7.01	Public Project Website, Flyer & Templates	Nov-13	confidential document, public deliverable
D8.01	Quality Assurance Plan (QAP)	Nov-13	confidential
D8.02	Internal Project website and internal IT communication infrastructure	Nov-13	confidential
D1.01	Specification Use Cases	Jan-14	restricted
D1.02	Attack Model	Jan-14	restricted
D1.03	Security Requirements	Apr-14	restricted
D4.01	Preliminary Security Model	Apr-14	public
D1.04	Common Reference Architecture	Jul-14	public
D5.01	Framework Architecture, Tool Flow and APIs	Jul-14	restricted
D2.01	Early White-Box Cryptography and Data Obfuscation Report	Oct-14	public
D2.02	Binary Code Splitting Support	Oct-14	confidential
D2.03	Binary Code Splitting & Obfuscation Report	Oct-14	public
D3.01	Preliminary Online Protections Report	Oct-14	public
D4.02	Preliminary Complexity Metrics	Oct-14	public
D5.02	ASPIRE Offline Compiler Tool Chain	Oct-14	confidential
D5.03	ASPIRE Offline Compiler Tool Chain Report	Oct-14	public
D6.01	Use Case Applications	Oct-14	confidential
D7.02	Dissemination Plan	Oct-14	public
D7.03	Preliminary Exploitation Plan	Oct-14	confidential
D8.03	Technical Periodic Project Report 1		
D8.04	Financial Periodic Project Report 1		
D2.04	White-box Crypto Library and Code Generation	May-15	confidential
D2.05	Binary Code Obfuscation Support	May-15	confidential
D2.06	Binary Code Obfuscation Report	May-15	Public
D3.02	Preliminary Online Protections Support	May-15	confidential
D5.04	ASPIRE Offline Protection Tool Chain	May-15	confidential
D2.07	Offline Code Protection Support	Oct-15	confidential
D2.08	ASPIRE Offline Code Protection Report	Nov-15	public
D3.03	Client-Server Splitting and Client Mobile Code Support	Nov-15	confidential
D3.04	Intermediate Online Protections Report	Nov-15	public
D4.03	Security Model, Knowledge Base, Human Experiments		
D5.05	Preliminary ASPIRE Online Protection Tool Chain		

NAVIGATION

- Publications
  - Papers
  - Project deliverables
  - Other resources
- Knowledge base

Figure 15 - Screenshot of the ASPIRE webpage with the list of deliverables

Due to a configuration issue that was not resolved until late May 2014, we can only present Google Analytics results for the period June 2014 – Nov 2016 (see Table 1).



	month	sessions	users	new users
2014	June	169	105	57.40%
	July	160	124	68.12%
	August	157	128	74.52%
	September	262	179	61.83%
	October	226	160	61.50%
	November	190	128	51.58%
	December	182	119	59.34%
2015	January	205	138	57.56%
	February	167	154	82.04%

	March	518	429	78.96%
	April	510	418	76.67%
	May	1,051	930	86.11%
	June	1,130	1,041	90.53%
	July	902	815	87.47%
	August	562	506	87.90%
	September	227	139	50.66%
	October	200	113	47.00%
	November	533	412	72.80%
	December	409	369	86.31%
2016	January	257	230	84.82%
	February	214	125	50.47%
	March	400	298	69.25%
	April	443	340	71.78%
	May	583	484	79.59%
	June	405	320	76.54%
	July	467	386	80.51%
	August	448	382	82.37%
	September	337	289	71.81%
	October	421	342	79.33%
	November	487	241	44.56%

Table 1: Google Analytics from ASPIRE website

As shown in Figure 16, which depicts the number of new users per country, the ASPIRE website draws worldwide attention.

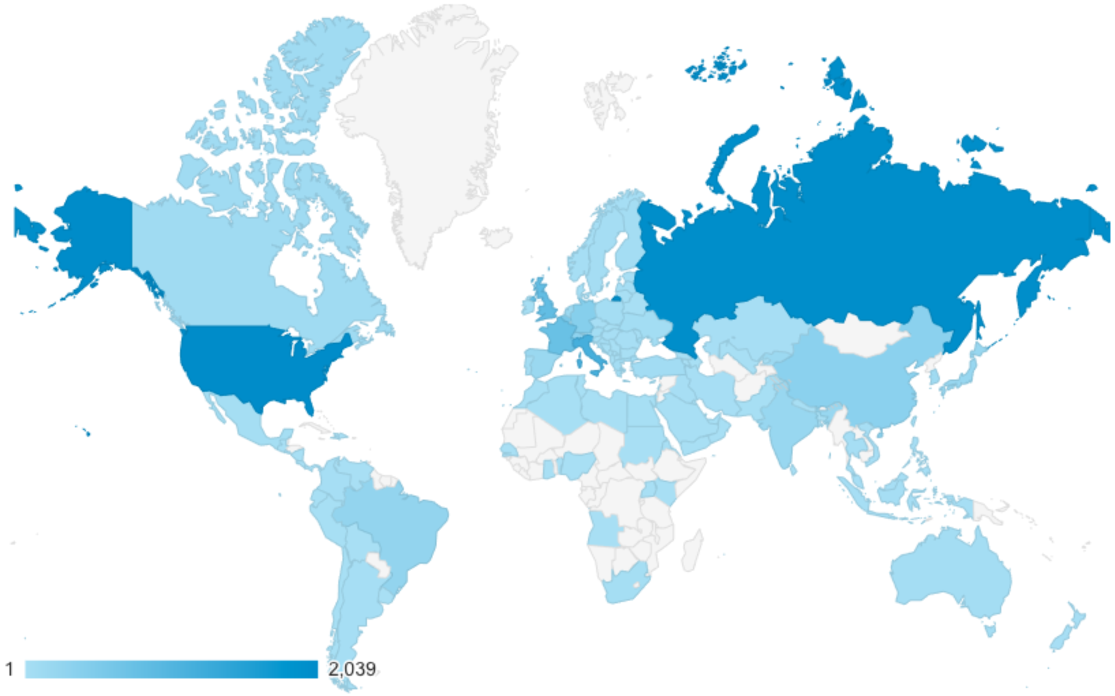


Figure 16 - Unique users per country visiting the ASPIRE website (June 2014 - Nov 2016)

2.1.2 Restricted Area of ASPIRE Website

As can be seen at the top of the screenshot in Figure 9, the ASPIRE website allows consortium members to register and log in to the website. After doing so, the private part of the website can be accessed.

This part includes:

- **wiki** pages used for internal dissemination of relevant information that needs to be updated regularly;
- a **Steering Board** page linking and listing all information regarding the boards' meetings, such as agendas and minutes;
- an **action tracker** page listing all ongoing actions, deadlines, progress states, etc.;
- **mailing list archives**;
- the project **SVN repository for documents**.
- the project **SVN repository for source code**.

2.2 Social Media

Social media can help in spreading project-related information to a wide audience. They are therefore a valuable tool to disseminate project ideas and results. To start using social media, we waited until enough results were becoming available, such that we can avoid so-called sleeping social media accounts.

In September 2014, the ASPIRE FP7 **Twitter** account was launched (https://twitter.com/aspirefp7), where project members can tweet about the project and related subjects.

In November 2014, the ASPIRE FP7 **LinkedIn** group was launched (https://www.linkedin.com/groups/Aspire-FP7-7300827), where stakeholders and other interested people will be.

2.3 YouTube Channel

In September 2016, the ASPIRE FP7 YouTube Channel was launched (https://www.youtube.com/channel/UCntMGBjHr_oW5wEd5JgjD6g). This channel shows about 30 video demonstrations of project results.

2.4 Open Sourcing

Part of the source code developed in the ASPIRE project have been open sourced. We also created an online presence for the open source parts of the project.

We decided to put all of our source code in git repositories. We created an ‘aspire-fp7’ team on the GitHub repository sharing website as the central point for our repositories, which can be found at https://github.com/aspire-fp7. The point of entry on this team is the ‘framework’ repository, which contains a set of links to all other open sourced ASPIRE git repositories.

As some partners need to track the number of downloads and clones of their open sourced materials, every protection technique is in a separate repository. Partners decide themselves where they want to host the repositories of their protection techniques. They can either put the repository on the central aspire-fp7 team, or on their own GitHub team page.

Most of the code written by the academic partners is open sourced. The only exception is are the source-to-source techniques developed by FBK, as they are planning to commercialize this technique in a spin-off. The ACTC, which is joint work between NAGRA, GTO, and UGent, has also been open sourced.

We have also written and published scripts to set up and to run Docker containers that contain all of the open sourced tools. Docker is a lightweight Linux virtualization technology. Rather than virtualize the entire operating system, containers merely isolate processes from the rest of the rest of the system. Containers are made of specific combinations of software versions, to allow for reproducibility. Users can thus clone our docker repository at https://github.com/aspire-fp7/docker, run the scripts, and immediately start running the ACTC on applications to apply both offline and online protections to applications.

On the ASPIRE website, we have added a new page that contains links to the open source repositories. We written documentation on how to set up the Docker container, how to run the ACTC and how to apply offline and online techniques to a demo application. This documentation is based on the ASPIRE Open Source Manual Deliverable D5.13.

Furthermore, we have open sourced and documented the ADSS Full at https://github.com/SPDSS/adss. We have also open sourced and documented the ADSS Light at https://github.com/uel-aspire-fp7/adss-light .

Section 3 Scientific Publications

Section Authors: Bjorn De Sutter (UGent), Paolo Falcarin, Elena Gómez-Martínez (UEL)

3.1 Peer-reviewed publications

1. Paolo Tonella, Mariano Ceccato, Bjorn De Sutter, Bart Coppens
A Measurement Framework to Quantify Software Protections (Poster + Extended Abstract)
Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014, p. 1505-1507, Scottsdale, Arizona (USA).

2. Bjorn De Sutter
Towards a Unified Framework for Evaluating the Strength of Software Protections (Extended Abstract)
Proc. of the ARO Workshop on Continuously Upgradeable Software Security and Protection, 2014, p. 34-35.

3. Brecht Wyseur
Reflections on Software Renewability from an Industry Perspective (Extended Abstract)
Proc. of the ARO Workshop on Continuously Upgradeable Software Security and Protection, 2014, p. 36-37.

4. Mariano Ceccato
On the Need for More Human Studies to Assess Software Protection (Extended Abstract)
Proc. of the ARO Workshop on Continuously Upgradeable Software Security and Protection, 2014, p. 55-56.

5. Biniam Fisseha Demissie, Mariano Ceccato, Roberto Tiella.
Assessment of data obfuscation with residue number coding.
In 2015 IEEE/ACM International Workshop on Software Protection, pages 38-44. IEEE, 2015.

6. Cataldo Basile, Daniele Canavese, Jerome D'Annoville, Bjorn De Sutter, Fulvio Valenza.
Automatic Discovery of Software Attacks via Backward Reasoning.
In 2015 IEEE/ACM International Workshop on Software Protection, pages 52-58. IEEE, 2015.

7. Bjorn De Sutter, Paolo Falcarin, Brecht Wyseur, Cataldo Basile, Mariano Ceccato, Jerome d'Annoville, Michael Zunke.
A reference architecture for software protection.
In 13th Working IEEE/IFIP Conference on Software Architecture. (WICSA), pages 291-294, April 2016.

8. Mariano Ceccato, Riccardo Scandariato.
Static Analysis and Penetration Testing from the Perspective of Maintenance Teams.
In Proceedings of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurements ESEM 2016. New York, NY, USA, 2016. ACM. pages 25:1-25:6

9. Mariano Ceccato, Paolo Falcarin, Alessandro Cabutto, Yosief Weldezghi Frezghi, Cristian-Alexandru Staicu.
Search Based Clustering for Protecting Software with Diversified Updates.
In Symposium on Search-Based Software Engineering SSBSE 2016. Springer. Pages 159-175.

10. Alessio Viticchié, Leonardo Regano, Marco Torchiano, Cataldo Basile, Mariano Ceccato, Paolo Tonella, Roberto Tiella.
Assessment of Source Code Obfuscation Techniques.
In IEEE International Working Conference on Source Code Analysis and Manipulation SCAM 2016. Pages 11-20.

11. Gaofeng Zhang, Paolo Falcarin, Elena Gómez-Martínez, Shareeful Islam, Christophe Tartary, Bjorn De Sutter, Jerome D'Annoville.
Attack simulation based software protection assessment method.
In International Conference On Cyber Security and Protection of Digital Services (Cyber Security 2016), Pages 1-8, IEEE, (Best paper Award).

12. Alessandro Cabutto, Paolo Falcarin, Bert Abrath, Bart Coppens, Bjorn De Sutter.
    Software Protection with Code Mobility.
    In Proceedings of the Second Workshop on Moving Target Defense MTD@CCS 2015, Pages 95-103, ACM.

13. Alessio Viticchié, Cataldo Basile, Andrea Avancini, Mariano Ceccato, Bert Abrath, Bart Coppens.
    Reactive attestation: Automatic detection and reaction to software tampering attacks.
    In *Proceedings of the 2016 ACM Workshop on Software PROtection* (SPRO 2016), pages 91-92, 2016, ACM.

14. Gaofeng Zhang, Paolo Falcarin, Elena Gómez-Martínez, Shareeful Islam, Christophe Tartary, Bjorn De Sutter, Jerome D'Annoville.
    Attack Simulation based Software Protection Assessment Method with Petri Net
    International Journal on Cyber Situational Awareness, Vol 1:1, ISSN 2057-2182 2016 (in press).

15. Bert Abrath, Joris Wijnant, Bart Coppens, Bjorn De Sutter, and Stijn Volckaert
    A Tightly-Coupled Self-Debugging Software Protection. Accepted for publication in 6th International Workshop on Software Security, Protection and reverse Engineering (SSPREW-2016), Springer, December 2016.

16. Roberto Tiella, Mariano Ceccato
    Automatic Generation of Opaque Constants Based on the K-clique Problem for Resilient Data Obfuscation.
    Accepted for publication in the 24th IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER-2017), IEEE.

17. Regano, Leonardo; Canavese, Daniele; Basile, Cataldo; Viticchié, Alessio; Lioy, Antonio (2016)
    Towards Automatic Risk Analysis and Mitigation of Software Applications.
    In: 10th IFIP WG 11.2 International Conference, WISTP 2016, Heraklion, Crete (Greece), September 26–27, 2016. pp. 120-135, Volume 9895 of the book series Lecture Notes in Computer Science (LNCS)

3.2 Other publications (not peer-reviewed)

1. Yosief Weldezghi Frezghi
   Code Diversity: Code Obfuscation and Clustering Heuristic to Prevent Code Tampering
   Master Thesis, University of Trento, Department of Information Engineering and Computer Science. Advisor: Luigi Palopoli, Second Supervisor: Mariano Ceccato. Academic Year 2013-2014

2. Biniam Fisseha Demissie
   Implementation and Assessment of Data Obfuscation for C/C++ Code Based on Residue Number Coding.
   Master Thesis, University of Trento, Department of Information Engineering and Computer Science. Advisor: Bruno Crispo, Second Supervisors: Mariano Ceccato and Roberto Tiella. Academic Year 2013-2014.

3. Bjorn De Sutter
   Evaluating the Strength of Software Protections (Abstract)
   Challenges in Analysing Executables: Scalability, Self-Modifying Code and Synergy, Report from Dagstuhl Seminar 14241, 2014, p. 54

4. Bjorn De Sutter
   Making Advanced Software Protection Tools Usable for Non-Experts
   In 2015 IEEE/ACM International Workshop on Software Protection, page 2. IEEE, 2015.

5. Alessandro Valentini
   An Experimental Study on Run-Time Overhead Introduced by Data Obfuscation Transformations
   Master Thesis, University of Trento, Department of Information Engineering and Computer Science. Advisor: Bruno Crispo, Second Supervisors: Roberto Tiella and Mariano Ceccato. Academic Year 2015-2016

6. Bjorn De Sutter, Cataldo Basile, Mariano Ceccato, Paolo Falcarin, Michael Zunke, Brecht Wyseur, and Jerome d'Annoville.
   The ASPIRE Framework for Software Protection.
   In *Proceedings of the 2016 ACM Workshop on Software PROtection* (SPRO '16), pp 91-92, 2016
7. Thomas Van Cleemput
   Automatische injectie van flexibele opake predicaten
   Master Thesis, Ghent University, June 2015
8. Joris Wijnant
   SAD Droid: Zelf-Anti-Debugging voor Android
   Master Thesis, Ghent University, Sept 2015

3.3 Future Publications Plan

Submitted but rejected papers will be revised and resubmitted again after the end of the project. Moreover, several papers are being prepared, including a new paper on the attack experiments with tiger teams, a paper on the code renewability framework (extending the MTD-15 workshop paper), a paper on crash reporting for diversified binaries, a paper on hiding the boundaries between the application and the linked-in protection components, a journal paper on maximizing software diversity (extending the SSBSE-16 conference paper), a paper on the ACTC tool flow, etc.

The confidential annex to this report lists the papers submitted but rejected during the course of the project.

Section 4 Face-to-Face Dissemination

Section Authors:

Bjorn De Sutter (UGent), Elena Gómez-Martínez (UEL)

4.1 Participations in Conference or Workshops

1.	Activity:	Conference
	Main Leader:	Bjorn De Sutter, UGent
	Title:	A Golden Standard for Evaluating Software Protection against Man-at-the-End Attacks
	Place:	Vienna (AU)
	Date:	20/01/2014
	Audience Size:	25
	Type and Goal Event:	Keynote speech at the Cryptography and Security in Computing Systems (CS^2) workshop (col. with the HiPEAC conference)
	Countries Addresses:	International
2.	Activity	Workshop
	Main Leader:	Paolo Falcarin, UEL and Bjorn De Sutter, UGent
	Title	Software Protection with Code Mobility
	Place	Denver (USA)
	Date	15/10/2015
	Audience Size	20
	Type and Goal Event	Accepted paper presentation
	Countries Addresses	International
3.	Activity	Presentation
	Main Leader:	Brecht Wyseur, NAGRA
	Title	White-Box Cryptography and Smart Cards: Friend or Foe?
	Place	Bochum (Germany)
	Date	4/11/2015
	Audience Size	100
	Type and Goal Event	Keynote at CARDIS 2015 conference
	Countries Addresses	International
4.	Activity	Workshop
	Main Leader:	Brecht Wyseur, NAGRA
	Title	NAGRA-EDSI Exploitation workshop
	Place	Rennes (France)
	Date	23/02/2016
	Audience Size	10
	Type and Goal Event	Exploitation workshop
	Countries Addresses	International
5.	Activity	Conference
	Main Leader:	Cataldo Basile POLITO and Mariano Ceccato, FBK
	Title	Assessment of Source Code Obfuscation Techniques
	Place	Raleigh, NC, USA
	Date	2/3/2016
	Audience Size	100
	Type and Goal Event	Paper presentation at "International Working Conference on Source Code Analysis and Manipulation" (SCAM-2016)
	Countries Addresses	International
6.	Activity	Conference
	Main Leader:	Paolo Falcarin, UEL
	Title	A reference architecture for software protection
	Place	Venice, Italy
	Date	7/4/2016

	Audience Size	30
	Type and Goal Event	Accepted paper presentation WICSA 2016 (industry track)
	Countries Addresses	International
7.	Activity	Conference
	Main Leader:	Paolo Falcarin, UEL
	Title	Attack Simulation based Software Protection Assessment Method for Protection Optimisation
	Place	London, United Kingdom
	Date	14/6/2016
	Audience Size	50
	Type and Goal Event	Accepted paper presentation at IEEE Cyber Security 2016 (Best paper award)
	Countries Addresses	International
8.	Activity	Poster
	Main Leader:	Paolo Falcarin, UEL
	Title	Software protection assessment with code metrics and petri nets
	Place	London, United Kingdom
	Date	16/6/2016
	Audience Size	100
	Type and Goal Event	ACE school showcase of students and research projects to local industry and politicians
	Countries Addresses	National
9.	Activity	Poster
	Main Leader:	Paolo Falcarin, UEL
	Title	Poster: A Light Process for the Software Protection Assessment Based On Petri Nets
	Place	Valencia, Spain
	Date	1/7/2016
	Audience Size	100
	Type and Goal Event	ACM Informática para todos http://acmupv.webs.upv.es/informatica-para-tods-2016/
	Countries Addresses	National
10.	Activity	Presentation
	Main Leader:	Brecht Wyseur, NAGRA
	Title	Talk at WhibOx workshop
	Place	Santa Barbara, California, USA
	Date	14/8/2016
	Audience Size	90
	Type and Goal Event	Keynote at a white-box and obfuscation workshop, co-located with CRYPTO
	Countries Addresses	International
11.	Activity	Conference
	Main Leader:	Mariano Ceccato, FBK
	Title	Static Analysis and Penetration Testing from the Perspective of Maintenance Teams
	Place	Ciudad Real, Spain
	Date	8/9/2016
	Audience Size	100
	Type and Goal Event	Paper presentation at "Symposium on Empirical Software Engineering and Measurements"
	Countries Addresses	International
12.	Activity	Conference
	Main Leader:	Cataldo Basile, POLITO
	Title	Towards Automatic Risk Analysis and Mitigation of Software Applications

	Place	Heraklion, Crete (Greece)
	Date	26/9/2016
	Audience Size	50
	Type and Goal Event	Workshop paper @ 10th IFIP WG 11.2 International Conference, WISTP 2016
	Countries Addresses	International
13.	Activity	Presentation
	Main Leader:	Paolo Falcarin, UEL
	Title	Software Protection seminar
	Place	Hangzhou, China
	Date	20/5/2016
	Audience Size	60
	Type and Goal Event	Overview of the ASPIRE project for Bachelor students and staff at Hangzhou Dianzi University (China)
	Countries Addresses	International
14.	Activity	Interview
	Main Leader:	Bjorn De Sutter, UGent
	Title	Locking the Back Door
	Place	Online
	Date	29/6/2016
	Audience Size	500
	Type and Goal Event	Written interview for a security special feature of the HiPEAC Info newsletter issue 48
	Countries Addresses	International
15.	Activity	Interview
	Main Leader:	Bjorn De Sutter, UGent
	Title	Combined protections for greater mobile app security
	Place	Online
	Date	9/9/2016
	Audience Size	
	Type and Goal Event	Written interview for an article on the CORDIS website
	Countries Addresses	International
16.	Activity	Workshop
	Main Leader:	Cataldo Basile, POLITO
	Title	Towards Automatic Risk Analysis and Mitigation of Software Applications
	Place	Heraklion, Crete (Greece)
	Date	26/9/2016
	Audience Size	50
	Type and Goal Event	Workshop paper @ 10th IFIP WG 11.2 International Conference, WISTP 2016
	Countries Addresses	International
17.	Activity	Conference
	Main Leader:	Mariano Ceccato, FBK and Paolo Falcarin, UEL
	Title	Search Based Clustering for Protecting Software with Diversified Updates
	Place	Raleigh, North Carolina (USA)
	Date	8/10/2016
	Audience Size	100
	Type and Goal Event	Paper presentation at Symposium on Search Based Software Engineering SSBSE-2016
	Countries Addresses	International
18.	Activity	Conference

Main Leader:	Andrea Avancini and Mariano Ceccato, FBK and Cataldo Basile Alessio Viticchié POLITO
Title	Reactive Attestation: Automatic Detection and Reaction to Software Tampering Attacks
Place	Vienna (Austria)
Date	28/10/2016
Audience Size	50
Type and Goal Event	Paper presentation at the 2nd International Workshop on Software Protection (SPRO-2016)
Countries Addresses	International

4.2 Presentations

1.	Activity:	Exhibition
	Main Leader:	Brecht Wyseur, NAGRA
	Title:	ASPIRE: Advanced Software Protection: Integration, Research and Exploitation
	Place:	Brussels (BE)
	Date:	28/03/2014
	Audience Size:	480
	Type and Goal Event:	Poster at the EU Cybersecurity Strategy - High Level Conference
	Countries Addresses:	International
2.	Activity:	Presentation
	Main Leader:	Paolo Falcarin, UEL
	Title:	Software Protection Research Overview
	Place:	London (UK)
	Date:	20/01/2014
	Audience Size:	20
	Type and Goal Event:	Internal presentation to research development team at UEL to plan for knowledge transfer and collaborations
	Countries Addresses:	National
3.	Activity:	Presentation
	Main Leader:	Cataldo Basile, POLITO
	Title:	ASPIRE: Advanced Software Protection: Integration, Research and Exploitation
	Place:	Torino (Italy)
	Date:	26/02/2014
	Audience Size:	15
	Type and Goal Event:	Internal presentation to the TORSEC group of Politecnico di Torino
	Countries Addresses:	National
4.	Activity:	Presentation
	Main Leader:	Cataldo Basile, POLITO
	Title:	ASPIRE: Advanced Software Protection: Integration, Research and Exploitation
	Place:	Torino (Italy)
	Date:	14/03/2014
	Audience Size:	20
	Type and Goal Event:	Internal presentation to SECURED team of the Politecnico di Torino
	Countries Addresses:	National
5.	Activity:	Presentation
	Main Leader:	Antonio Lioy, POLITO
	Title:	ASPIRE: Advanced Software Protection: Integration, Research and Exploitation
	Place:	Torino (Italy)
	Date:	5/12/2013
	Audience Size:	150
	Type and Goal Event:	Presentation of the ASPIRE project to the Master students of the course

03GSD “Sicurezza dei sistemi informatici” (Computer systems security)
Countries Addresses: National

6. Activity: Presentation
Main Leader: Antonio Lioy, POLITO
Title: ASPIRE: Advanced Software Protection: Integration, Research and Exploitation
Place: Torino (Italy)
Date: 9/12/2013
Audience Size: 100
Type and Goal Event: Presentation of the ASPIRE project to the Master students of the course 02KRQ “Computer System Security”
Countries Addresses: National

7. Activity: Presentation
Main Leader: Paolo Falcarin, UEL
Title: Software Protection
Place: London (UK)
Date: 30/04/2014
Audience Size: 20
Type and Goal Event: UEL Expert Series: academics are invited to present their work to audience of small-medium enterprises
Countries Addresses: National

8. Activity: Presentation
Main Leader: Mariano Ceccato, FBK
Title: Code Diversity: Code Obfuscation and Clustering Heuristic to Prevent Code Tampering
Place: Trento (IT)
Date: 12/03/2014
Audience Size: 30
Type and Goal Event: Master thesis defenced by Yosief Weldezghi Frezghi, under supervision of Mariano Ceccato
Countries Addresses: National

9. Activity: Interview
Main Leader: Bjorn De Sutter, UGent
Title: The ASPIRE project
Place: -
Date: 30/04/2014
Audience Size:
Type and Goal Event: Published in the EU Yearbook, which was compiled by the team of the EU FP7 project SecCord (http://www.seccord.eu)
Countries Addresses: International

10. Activity: Presentation
Main Leader: Bjorn De Sutter, UGent
Title: Evaluating the strength of software protections
Place: Dagstuhl (DE)
Date: 11/06/2014
Audience Size: 44
Type and Goal Event: Dagstuhl Seminar on "Challenges in Analysing Executables: Scalability, Self-Modifying Code and Synergy"
Countries Addresses: International
URL: http://www.dagstuhl.de/en/program/calendar/semhp/?semnr=14241

11. Activity: Lecture
Main Leader: Bjorn De Sutter, UGent
Title: Evaluating the strength of software protections
Place: Verona (IT)
Date: 30/07/2014
Audience Size: 35

Type and Goal Event: Lecture of 3 hours at ISSISP Summer School on Software Protection,
Countries Addresses: International
URL: http://issisp2014.di.univr.it/

12. Activity: Lecture
Main Leader: Brecht Wyseur, NAGRA
Title: White-box Cryptography
Place: Verona (IT)
Date: 28/07/2014
Audience Size: 35
Type and Goal Event: Lecture of 3 hours at ISSISP Summer School on Software Protection,
Countries Addresses: International
URL: http://issisp2014.di.univr.it/

13. Activity: Presentation
Main Leader: Jens Van den Broeck, UGent
Title: The ASPIRE project
Place: Verona (IT)
Date: 31/07/2014
Audience Size: 35
Type and Goal Event: Poster presentation at ISSISP Summer School on Software Protection,
Countries Addresses: International
URL: http://issisp2014.di.univr.it/

14. Activity: Presentation
Main Leader: Brecht Wyseur, NAGRA
Title: An introduction to ASPIRE
Place: Cheseaux, CH
Date: 10/09/2014
Audience Size: 50
Type and Goal Event: Brecht presented the project to NAGRA's group-wide security experts

15. Activity: Presentation
Main Leader: Brecht Wyseur, NAGRA
Title: The ASPIRE use case demonstrator
Place: Cheseaux, CH
Date: 11/09/2014
Audience Size: 20
Type and Goal Event: Presentation during company internal Technical Session Workshop

16. Activity: Presentation
Main Leader: Mariano Ceccato, FBK
Title: Implementation and Assessment of Data Obfuscation for C/C++ Code Based on Residue Number Coding
Place: Trento (IT)
Date: 14/10/2014
Audience Size: 30
Type and Goal Event: Master thesis defenced by Biniam Fisseha Demissie, under supervision of Mariano Ceccato
Countries Addresses: National

17. Activity Theses
Main Leader: Roberto Tiella, FBK
Title An Experimental Study on Run-Time Overhead Introduced by Data Obfuscation Transformations
Place Trento (Italy)
Date 24/3/2016
Audience Size
Type and Goal Event Master thesis defenced by Alessandro Valentini, under supervision of Roberto Tiella and Mariano Ceccato
Countries Addresses National

18.	Activity	Theses
	Main Leader:	Cataldo Basile, Antonio Lioy, POLITO
	Title	Attestazione remota basata su controllo di invarianti
	Place	Torino (Italy)
	Date	December/2015
	Audience Size	
	Type and Goal Event	Master thesis defenced by Daniele Cortis under supervision of Cataldo Basile and Antonio Lioy
	Countries Addresses	National
19.	Activity	Presentation
	Main Leader:	Paolo Falcarin, UEL
	Title	Software protection seminar - ASPIRE overview
	Place	Milano (Italy)
	Date	2/12/2014
	Audience Size	50
	Type and Goal Event	Scientific Community. Guest lecture within the Master on Reverse Engineering at Universitá di Milano-Bicocca, in front of staff and students of Master in Reverse Engineering
	Countries Addresses	National
20.	Activity	Presentation
	Main Leader:	Cataldo Basile, Antonio Lioy, POLITO
	Title	Modellazione di protezioni software attraverso ontologie formali
	Place	Torino (Italy)
	Date	December/2014
	Audience Size	
	Type and Goal Event	Master thesis defenced by Piepaolo Penna, under supervision of Cataldo Basile and Antonio Lioy
	Countries Addresses	National
21.	Activity	Theses
	Main Leader:	Cataldo Basile, POLITO
	Title	Modellazione di protezioni software attraverso ontologie formali
	Place	Torino (Italy)
	Date	December/2014
	Audience Size	
	Type and Goal Event	Master thesis defenced by Piepaolo Penna, under supervision of Cataldo Basile and Antonio Lioy
	Countries Addresses	National
22.	Activity	Exhibition
	Main Leader:	Bjorn De Sutter, UGent
	Title	ASPIRE Booth and Poster at the Cybersecurity & Privacy Innovation Forum
	Place	Brussels, Belgium
	Date	28-29/01/2015
	Audience Size	400
	Type and Goal Event	A two-day networking event with presentations/presence of EC-funded cyber security & privacy research, see https://ec.europa.eu/digital-agenda/en/news/cybersecurity-privacy-innovation-forum
	Countries Addresses	International
23.	Activity	Presentation
	Main Leader:	Bjorn De Sutter, UGent
	Title	Making Advanced Software Protection Tools Usable for Non-Experts
	Place	Firenze (Italy)
	Date	18/5/2015
	Audience Size	43
	Type and Goal Event	Keynote at software protection workshop by project coordinator
	Countries Addresses	International
24.	Activity	Presentation

Main Leader:	Bjorn De Sutter, UGent
Title	System Software Lab Research Overview
Place	Gent (Belgium)
Date	21/4/2015
Audience Size	40
Type and Goal Event	Overview of the project for Bachelor and Master students UGent
Countries Addresses	National

25.

Activity	Theses
Main Leader:	Cataldo Basile, Antonio Lioy, POLITO
Title	Attestazione remota del software
Place	Torino (Italy)
Date	March/2015
Audience Size	
Type and Goal Event	Master thesis defenced by Alessio Viticchié under supervision of Cataldo Basile and Antonio Lioy
Countries Addresses	National

26.

Activity	Presentation
Main Leader:	Bjorn De Sutter, UGent
Title	ASPIRE project presentation
Place	Gent (Belgium)
Date	8/6/2016
Audience Size	1
Type and Goal Event	Presentation of project to Vikram Adve, main LLVM development leader
Countries Addresses	International

27.

Activity	Theses
Main Leader:	Bjorn De Sutter, UGent
Title	Automatische injectie van flexibele opake predicaten
Place	Gent (Belgium)
Date	23/6/2016
Audience Size	
Type and Goal Event	Master thesis defenced by Thomas Van Cleemput, under supervision of Bjorn De Sutter
Countries Addresses	National

28.

Activity	Theses
Main Leader:	Bjorn De Sutter, UGent
Title	SAD Droid: Zelf-Anti-Debugging voor Android
Place	Gent (Belgium)
Date	4/9/2016
Audience Size	
Type and Goal Event	Master thesis defenced by Joris Wijnant, under supervision of Bjorn De Sutter
Countries Addresses	National

29.

Activity	Presentation
Main Leader:	Mariano Ceccato, FBK
Title	ASPIRE - Trustworthy software execution on untrusted mobile platforms
Place	Luxembourg (Luxembourg)
Date	10/9/2015
Audience Size	30
Type and Goal Event	Invited talk
Countries Addresses	National

30.

Activity	Poster Presentation
Main Leader:	Bjorn De Sutter, UGent
Title	ASPIRE poster. Available at: https://www.youtube.com/watch?v=A802IPCVAuQ

	Place	European Project Poster Session at the HiPEAC 2015 conference Amsterdam (Netherlands)
	Date	19-21/1/2016
	Audience Size	500
	Type and Goal Event	Poster
	Countries Addresses	International
31.	Activity	Poster Presentation
	Main Leader:	Bjorn De Sutter, UGent
	Title	ASPIRE poster
	Place	HiPEAC 2016 conference, Prague (Czech Republic)
	Date	18-20/1/2016
	Audience Size	500
	Type and Goal Event	Poster
	Countries Addresses	International
32.	Activity	Presentation
	Main Leader:	Bart Coppens and Bert Abrath, UGent
	Title	ASPIRE Tool Demonstration
	Place	Kudelski Headquarters, Cheseaux-sur-Lausanne (France)
	Date	8/3/2016
	Audience Size	
	Type and Goal Event	
	Countries Addresses	International
33.	Activity	Presentation
	Main Leader:	Bjorn De Sutter, UGent
	Title	ASPIRE: Advanced Software Protection: Integration, Research, and Exploitation
	Place	Gent, Belgium
	Date	18/10/2016
	Audience Size	
	Type and Goal Event	Presentation to the Belgian OWASP chapter meeting
	Countries Addresses	National
34.	Activity	Tutorial
	Main Leader:	Bjorn De Sutter, UGent and Cataldo Basile, POLITO
	Title	The ASPIRE Framework for Software Protection
	Place	Austria
	Date	28/10/2016
	Audience Size	50
	Type and Goal Event	Tutorial on ASPIRE framework in the SPRO workshop
	Countries Addresses	International
35.	Activity	Presentation
	Main Leader:	Paolo Falcarin, UEL
	Title	ASPIRE: Advanced Software Protection: Integration, Research and Exploitation
	Place	London (UK)
	Date	31/10/2016
	Audience Size	25
	Type and Goal Event	Presentation of ASPIRE project to Master students of the course CN7016 “Computer Security”
	Countries Addresses	National

4.3 Upcoming Events

1.	Activity	Presentation

Main Leader:	Bert Abrath, UGent
Title	Tightly-Coupled Self-Debugging Software Protection
Place	Los Angeles, USA
Date	6/12/2016
Audience Size	TBA
Type and Goal Event	Paper at 6th International Workshop on Software Security, Protection and reverse Engineering (SSPREW-2016)
Countries Addresses	International

Section 5 Workshops

Section Authors:

Paolo Falcarin (UEL), Brecht Wyseur (NAGRA)

5.1 1st International Workshop on Software PROtection

The initial plan was to co-locate the workshop with a major event in Europe, but in 2015 all the potential top security conferences were not in Europe, thus we aimed at a software engineering conference to reach out to the wide software engineering community.

The first Software PROtection (SPRO) workshop was co-located with the ACM/IEEE International Conference on Software Engineering (ICSE) in Florence (Italy) on 19th May 2015, one of the three top conferences in software engineering.

The website banner of the workshop (see Figure 17) was created by UEL by extending with a security flavour the main ICSE "Renaissance" theme, and adding to the Botticelli's Venus an espresso cup (as "spro" is an abbreviation of "espresso" in some American slang, according to www.urbandictionary.com).

SPRO 2015
May, 19th 2015 - ICSE - Florence, Italy
1st International Workshop on
Software PROtection
PASSWORD

Figure 17- The First SPRO website banner.

In this workshop, Paolo Falcarin served as general chair and Brecht Wyseur served as program chair. They first assembled and submitted a proposal for a workshop to the ICSE workshops chairs, and after the workshop proposal was accepted, they assembled the program committee (in which all ASPIRE Principal Investigators were involved), and launched the workshop website at https://aspire-fp7.eu/spro/.

The SPRO-2015 Programme Committee was formed by the following experts:

- Jerome d'Annoville – Gemalto, France
- Jean Daniel Aussel – Gemalto, France
- Cataldo Basile – Politecnico di Torino, Italy
- Mariano Ceccato – Fondazione Bruno Kessler, Italy
- Christian Collberg – University of Arizona, USA
- Bart Coppens – Ghent University, Belgium
- Mila Dalla Preda – University of Verona, Italy
- Koen De Bosschere – Ghent University, Belgium
- Saumya Debray – University of Arizona, USA
- Bjorn De Sutter – Ghent University, Belgium
- Werner Dondl – SafeNet Inc., USA/Germany
- Michael Franz – University of California, Irvine, USA
- Roberto Giacobazzi – University of Verona, Italy

- Yuan Gu – Irdeto
- Wulf Harder – SIA QuBalt, Latvia
- Pascal Junod – HEIG-VD, Switzerland
- Johannes Kinder – Royal Holloway Univ. of London, UK
- Antonio Lioy – Politecnico di Torino, Italy
- Isabella Mastroeni – University of Verona, Italy
- Christian Mönch – Conax, Norway
- Mattia Monga – University of Milan, Italy
- Riccardo Scandariato – Chalmers University, Sweden
- Christophe Tartary – University of East London, UK
- Clark Thomborson – University of Auckland, New Zealand
- Paolo Tonella – Fondazione Bruno Kessler, Italy
- Gaofeng Zhang – University of East London, UK
- Michael Zunke – SafeNet Inc., USA/Germany

The Programme committee followed a very thorough review process to ensure high quality papers and presentations. Each research paper was reviewed by at least four program committee members. We received 19 submissions from 60 authors of 13 countries. The nine best papers were accepted as full papers for publication and presentation at the workshop; of the accepted papers, 12 authors were from industry and 18 from academia.

Five of the nineteen papers submitted came from the ASPIRE consortium, and three of them were accepted. About 40 people registered for the workshop, coming from North America, Europe, and Asia.

We also included in the final workshop programme two keynote talks: one from Professor Bart Preneel in the morning and one from Professor Bjorn De Sutter in the afternoon. The first keynote from Professor Preneel provided an overview of the challenging problems faced by software security, while the second keynote from Professor De Sutter presented the ASPIRE initial results, and introduced the overall aims and objectives of the ASPIRE framework.

The final workshop programme was as follows:

- 09:00 Welcome + opening by program chair Brecht Wyseur

1st Keynote Talk (9.10-10.00)

- 09:10 **Keynote 1: "Software Security: Squaring the Circle" by Professor Bart Preneel** (KU Leuven and iMinds, Belgium).

Session 1: Research Papers: ***Software Protection Techniques*** *(10:00-12:30)*
Chair: Mariano Ceccato (Fondazione Bruno Kessler)

- 10:00 **Obfuscator-LLVM – Software Protection for the Masses**; Pascal Junod (HEIG-VD), Julien Rinaldini (HEIG-VD), Johan Wehrli (HEIG-VD) and Julie Michielin (Kudelski Security)

Coffee break (10:30-11:00)

- 11:00 Matryoshka: **Strengthening Software Protection via Nested Virtual Machines**; Sudeep Ghosh (Microsoft Corp.), Jason Hiser (University of Virginia) and Jack Davidson (University of Virginia)

- 11:30 **Using Virtual Machine Protections to Enhance Whitebox Cryptography**; Joseph Gan (V-Key), Roddy Kok (V-Key), Pankaj Kohli (V-Key), Dr. Yun Ding (V-Key) and Benjamin Mah (V-Key)
- 12:00 **Obfuscating Windows DLLs**; Bert Abrath (Ghent University), Bart Coppens (Ghent University), Stijn Volckaert (Ghent University) and Bjorn De Sutter (Ghent University).

Lunch break (12:30-14:00)

2nd Keynote Talk (14:00-15:00)

14:00 **Keynote 2: "Making Advanced Software Protection Tools Usable (for Non-Experts) by Professor Bjorn De Sutter** (Ghent University, Belgium).

*Session 2: Research Papers: **Software Protection Evaluation** (15:00-16:00)*
Chair: *Christian Mönch* (Conax)

- 15:00 **Code Artificiality: A Metric for the Code Stealth Based on an N-gram Model**; Yuichiro Kanzaki (National Institute of Technology, Kumamoto College), Akito Monden (Nara Institute of Science and Technology) and Christian Collberg (University of Arizona).
- 15:30 **Assessment of Data Obfuscation with Residue Number Coding**; Biniam Fisseha Demissie (Fondazione Bruno Kessler), Mariano Ceccato (Fondazione Bruno Kessler) and Roberto Tiella (Fondazione Bruno Kessler).

Coffee break (16:00-16:30)

*Session 3: **Formal Methods for Software Protection** (16:30-18:00)*
Chair: Jack Davidson (University of Virginia)

- 16:30 **Infections as Abstract Symbolic Finite Automata: Formal Model and Applications**; Mila Dalla Preda (University of Verona) and Isabella Mastroeni (University of Verona).
- 17:00 **Automatic discovery of software attacks via backward reasoning**; Cataldo Basile (Politecnico di Torino), Daniele Canavese (Politecnico di Torino), Jerome d'Annoville (Gemalto), Bjorn De Sutter (Ghent University) and Fulvio Valenza (Politecnico di Torino).
- 17:30 **A Framework for Measuring Software Obfuscation Resilience against Automated Attacks**; Sebastian Banescu (Technische Universität München), Martín Ochoa (Technische Universität München) and Alexander Pretschner (Technische Universität München).

At the end of the workshop, the organizers also announced their intention to keep organizing the SPRO workshop in the next year.

The workshop ended with a dinner sponsored by NAGRA, to which all attendants could participate if they registered. In the end, about 30 people attended the dinner, resulting in long and interesting discussions for the ASPIRE partners and the attendees on software security research.

5.2 2nd International Workshop on Software PROtection

The second SPRO workshop was co-located with the ACM CSS conference in Vienna on 28 October 2016, one of the three tier-1 conferences in the domain of computer security.

Figure 18 - The SPRO'16 banner

The initial plan was to co-locate the workshop with the HiPEAC conference in January 2016, but the potential of co-locating with ACM CSS, now that it was organized in Europe, was considered much greater. Moreover, the date ensured that the paper submission period would not overlap with that of the PPREW (now SSPREW, see http://www.pprew.org/) workshop, which targets the same authors and audience, albeit in the US.

For the second workshop, Brecht Wyseur served as general chair and Bjorn De Sutter served as program chair. They first assembled and submitted a proposal for a workshop to the ACM workshop chairs, and after the workshop proposal was accepted, they assembled the 25-person program committee (including ASPIRE Principal Investigators), and launched the workshop website at https://aspire-fp7.eu/spro/.

The SPRO-2016 Programme Committee was formed by the following experts:

- Andrea Höller -TU Graz, Austria
- Arun Lakhotia – University of Louisiana at Lafayette, USA
- Babak Yadegari – University of Arizona, USA
- Bart Coppens – Ghent University, Belgium
- Cataldo Basile – Politecnico di Torino, Italy
- Christian Collberg – University of Arizona, USA
- Christian Mönch – Conax, Norway
- Clark Thomborson – University of Auckland, New Zealand
- Frank Piessens -KU Leuven, Belgium
- Jack Davidson – University of Virginia, USA
- Jerome d'Annoville -Gemalto, France
- Johannes Kinder – Royal Holloway University of London, UK
- Karine Heydemann -Université Pierre et Marie Curie, Paris
- Mariano Ceccato – Fondazione Bruno Kessler, Italy
- Michael Franz – University of California Irvine, USA
- Mila Dalla Preda – University of Verona, Italy
- Paolo Falcarin – University of East London, UK
- Pascal Junod – HEIG-VD, Switzerland
- Roberto Giacobazzi – University of Verona, Italy
- Yuan Gu, Irdeto – USA
- Wulf Harder – QuBalt GmbH, Germany

Fourteen papers were submitted, of which three from within the ASPIRE consortium. Of those, eight papers were accepted, of which one from within the ASPIRE consortium.

The final workshop programme was as follows:

- 08:30 Welcome + opening by general chair Brecht Wyseur

Session 1: Keynote Talk (8:35-9:30)

- 08:35 **Keynote: Intel Software Guard Extensions – Introduction and Open Research Challenges by Dr. Matthias Schunter** (Intel Collaborative Research Institute for Secure Computing and Intel Labs).

*Session 2: Research Papers: **Vulnerabilities** (9:30-10:30)*
Chair: Mariano Ceccato (Fondazione Bruno Kessler)

- 09:30 **Beyond the Attack Surface: Assessing Security Risk with Random Walks on Call Graphs**; Nuthan Munaiah and Andrew Meneely (Rochester Institute of Technology).
- 10:00 **ROP Gadget Prevalence and Survival under Compiler-based Binary Diversification Schemes**; Joel Coffman, Daniel Kelly, Christopher Wellons and Andrew Gearhart (Johns Hopkins University Applied Physics Laboratory).

Coffee break (10:30-11:00)

Session 3: Research Papers: Obfuscation (11:00-12:30)
Chair: Johannes Kinder (Royal Holloway, University of London)

- 11:00 **Defeating MBA-based Obfuscation**; Ninon Eyrolles (Quarkslab), Louis Goubin (UVSQ, Laboratoire de mathématiques) and Marion Videau (Quarkslab and LORIA).
- 11:30 **VOT4CS: A Virtualization Obfuscation Tool for C#**; Sebastian Banescu, Ciprian Lucaci, Benjamin Kraemer and Alexander Pretschner (Technische Universität München).
- 12:00 **Binary Permutation Polynomial Inversion and Application to Obfuscation Techniques**; Lucas Barthélémy (Quarkslab and UPMC), Ninon Eyrolles (Quarkslab), Guenaël Renault and Raphaël Roblin (UPMC).

Lunch break (12:30-14:00)

Session 4: Research Papers: WBC & Integrity (14:00-15:30)
Chair: Christian Mönch (Conax)

- 14:00 **StIns4CS: A State Inspection Tool for C#**; Amjad Ibrahim and Sebastian Banescu (Technische Universität München).
- 14:30 **Reactive Attestation: Automatic Detection and Reaction to Software Tampering Attacks**; Alessio Viticchié (Politecnico di Torino), Andrea Avancini, Mariano Ceccato (Fondazione Bruno Kessler), Cataldo Basile (Politecnico di Torino), Bert Abrath, Bart Coppens (Ghent University).
- 15:00 **Attacking White-Box AES Constructions**; Brendan McMillion and Nick Sullivan (CloudFlare).

Coffee break (15:30-16:00)

Session 5: Panel Discussion (16:00-16:40)
Chair & Moderator: Brecht Wyseur, (Nagravision)

- 16:00 **Software Protection Research in Europe, where are we going?** Panel Members: Michael Zunke (SafeNet), Johannes Kinder (Royal Holloway, University of London), Nick Sullivan (Cloudflare), Clifford Liem (Cloakware/Irdeto)

Session 6: Tutorial (16:40-18:00)

- 16:40 **The ASPIRE Framework for Software Protection**; Bjorn De Sutter (Ghent University), and Cataldo Basile (Politecnico di Torino).

About 80 people registered for the workshop, coming from North America, Europe, Asia, and the Middle East. The vast majority of the registered attendants did show up, with the peak attendance being about 55 people.

The tutorial proved a great way to disseminate the ASPIRE outcomes, and to introduce the ongoing open-source effort and the publication of demonstration videos on the project's Youtube channel.

The panel discussion focused on answering the following questions:

- Observation 1: there's quite a big gap between industry needs and what academia is doing. How can we improve the collaboration between industry and academia?
- Observation 2: Quite some companies don't want to publish or disclose what they do, and are even reluctant to work with academia or give academia the right directions. There's quite some obscurity. (Up to some extent this is related to the previous question). How does this impact your job? How can we address this issue?
- Observation 3: In industry, it is hard for security researchers to explain to their management how secure things are or make comparison between different techniques on different products in different threat scenario's. At the same time, academics have difficulties with comparing technologies and validating / quantifying them. What is your experience with this? How do you and your colleagues tackle this issue? How can this issue be address more generally, e.g., via some better methodology / framework / …?

Some broadly supported statements made during the panel discussion were the following:

- It would be positive for the collaboration between academia and industry of academia would open source more prototype implementations.
- One of the most important aspects where academia should focus on is metrics for assessing protection strength.

At the end of the panel discussion, the workshop organizers also announced their intention to keep organizing the SPRO workshop in the years to come, and people were invited to join the SPRO steering committee. If possible, the workshop will be aligned with other efforts in the new H2020 EC PPP on Cyber Security and the activities of the new European Cyber Security Organization (ECSO, http://www.ecs-org.eu/). Offers to join forces with PPREW/SSPREW were discussed, but they were considered suboptimal: bringing together European software protection industry experts and academics will only be successful when done within Europe.

The workshop ended with a dinner sponsored by NAGRA, to which all attendants could participate if they registered. In the end, about 30 people attended the dinner, resulting in long and interesting discussions of many topics relevant to the workshop and to the ASPIRE partners and research.

Section 6 Public General Dissemination

Section Authors:

Bjorn De Sutter (UGent)

6.1 Web, Press Releases, Articles in Popular Press, TV Footage

1.

Activity:	Web
Main Leader:	UGent
Title:	ASPIRE Public Website
Date:	01/11/2013
Audience Size:	-
Type and Goal Event:	Website goes online
Countries Addresses:	International
URL:	https://www.aspire-fp7.eu/

2.

Activity:	Press Release
Main Leader:	UGent
Title:	Gentse onderzoekers ontwikkelen sterke bescherming voor mobiele software en diensten.
Date:	04/11/2013
Type and Goal Event:	Online press release
Countries Addresses:	Belgium

This press release is taken up on other news sites, including the Student Paper of Ghent University[1], Engineeringnet.be[2] and the news page of the Faculty of Engineering and Architecture of UGent[3].

3.

Activity:	News Report on Television
Main Leader:	Bjorn De Sutter, UGent
Title:	AVS News - The ASPIRE Project
Date:	05/11/2013
Audience Size:	-
Type and Goal Event:	The coordinator was interviewed, most of the interview was broadcasted on the local television station AVS in the province of Eastern Flanders in Belgium. The interview was mixed with information about the project, and footage taken during the project kick-off meeting. The whole report/news item lasted 2.18 minutes. A screenshot is shown in Figure 19.
Countries Addresses:	Belgium

4.

Activity:	Web
Main Leader:	UEL
Title:	€460,000 to develop software protection
Date:	01/12/2013
Audience Size:	-
Type and Goal Event:	ASPIRE project is presented on UEL website

[1] Press-release: http://www.schamper.ugent.be/2013-online/aspire-is-watching-you
[2] Engineeringnet.be http://engineeringnet.be/belgie/detail_belgie.asp?Id=11280&titel=Gentse%20onderzoekers%20zetten%20tanden%20in%20mobiele%20databescherming&category=nieuws
[3] Link no longer available online.

Countries Addresses:	UK
URL:	http://www.uel.ac.uk/research/news/aspire/

5.

Activity:	Web
Main Leader:	GTO
Title:	The ASPIRE F7 project
Date:	06/12/2013
Audience Size:	Company
Type and Goal Event:	Wiki page on the Gemalto Intranet describing the project and expected results

6.

Activity:	Web
Main Leader:	NAGRA
Title:	The ASPIRE F7 project
Date:	13/03/2014
Audience Size:	Company, 3000+
Type and Goal Event:	a post describing ASPIRE project has been published on Nagravision intranet's blog

7.

Activity:	Press Release
Main Leader:	Bjorn De Sutter, UGent
Title:	ASPIRE project to bring strong software protection to mobile devices
Date:	18/04/2014
Audience Size:	100k
Type and Goal Event:	International Press Release about the ASPIRE project.
Countries Addresses:	International

While the project started in Nov 2013, this press release was only released in April 2014 because it took a very long time to get the marketing departments of the project's industrial partners to agree on a text in which their principal investigators are quoted. Such quotations were preferred quite strongly, because or experience is that they make it much more likely that the press release is picked up by various news sites.

This news release was released via the Cordis Wire (http://cordis.europa.eu, published 17/4/2014) and AlphaGalileo (http://www.alphagalileo.org/ViewItem.aspx?ItemId=141251&CultureCode=en). Moreover, we contacted our contact persons at ACM to ensure that the news was picked up by ACM TechNews, the most broadly spread news forum in the computing systems domain, reaching an audience of over hundred thousand readers. The press release was indeed picked up by ACM TechNews in its news bulletin of 25/04/2014 (http://technews.acm.org/archives.cfm?fo=2014-04-apr/apr-25-2014.html#720483).

8.

Activity:	Press Release
Main Leader:	Bjorn De Sutter, UGent
Title:	ASPIRE and Cyber Security
Date:	08/05/2014
Audience Size:	-
Type and Goal Event:	Short presentation of the ASPIRE project submitted to, and released by the European Cyber Security Round Table in their Cyber Newsflash.
Countries Addresses:	International
URL:	http://www.security-round-table.eu

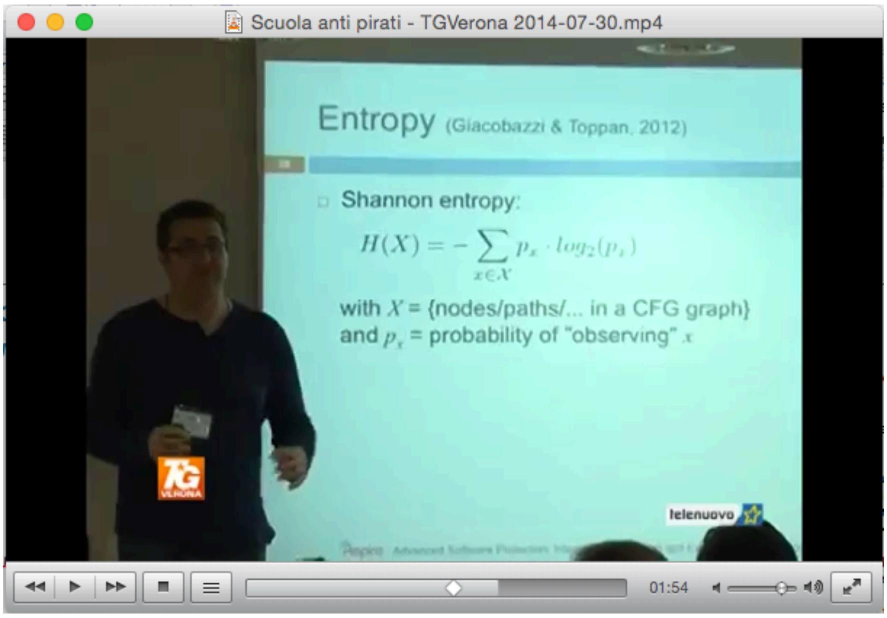
9.

Activity:	Press Release
Main Leader:	Bjorn De Sutter, UGent
Title:	FP7 ASPIRE Project
Date:	07/2014
Audience Size:	-
Type and Goal Event:	Presentation of the project in the "In the Spotlight" section of HiPEAC info 39, the 39th issue of the newsletter of the FP7 HiPEAC Network of Excellence
Countries Addresses:	International

URL: http://www.hipeac.net/content/hipeacinfo-39-july-2014

10. Activity: News Report on Television
Main Leader: Bjorn De Sutter, UGent
Title: Scuola anti pirati
Date: 30/07/2014
Audience Size: -
Type and Goal Event: A news report on local Italian television station TGVerona included fragments from Bjorn De Sutter's lecture on ASPIRE's software protection evaluation methodology. The whole report was 3.30 minutes long. See the screenshot in
Countries Addresses: Italy

Figure 19 - Screenshot local television interview/report on AVS



Entropy (Giacobazzi & Toppan, 2012)

- Shannon entropy:

$$H(X) = -\sum_{x \in X} p_x \cdot log_2(p_x)$$

with X = {nodes/paths/... in a CFG graph}
and p_x = probability of "observing" x

Figure 20 - Screenshot local television report on TGVerona

11. Activitiy: NAGRA-internal Press Release
Main Leader: Brecht Wyseur; NAGRA
Title: Pasta, Minestrone, and Software Protection
Date: October 2015
Audience Size: 3500

Type and Goal:	A press release in NAGRA in-house magazine on first SPRO workshop.
Countries Addressed:	International

Section 7 Cooperation with Other Projects

Section Authors:

Bjorn De Sutter (UGent), Cataldo Basile (Polito), Brecht Wyseur (NAGRA)

7.1 Activities

UGent collaborated with the TETRACOM FP7 project (http://www.tetracom.eu) to further prepare its IP for exploitation by an industrial partner, as documented more extensively in deliverable D7.03.

UGent's ASPIRE team also provides input to the vision building processes in the HiPEAC Network of Excellence (http://www.hipeac.net), in particular for drafting the HiPEAC vision documents and roadmaps on compiler technology and their use for protecting and securing software and computer systems.

Furthermore, the project coordinator has been active in the Digital Asset Protection Association (DAPA) project/organization (http://www.digitalassetprotectionassociation.org/), where he has been working with the scientific board members to draft a whitepaper on best practices for publishing and evaluation software protection papers and results. That work is of course heavily influenced by the methodology developed in WP4 of the ASPIRE project. Unfortunately, the DAPA has been a sleeping organization lately.

Within POLITO, there is a collaboration between the ASPIRE researchers and the researchers of the SECURED project. The SECURED project needs to remotely attest the software that has to execute the user security applications. Currently, the preferred approach is the TCG-based one, which uses secure hardware, i.e., the TPM, as root core of trust. We have checked together the requirements in both projects and examined the cases where a physical TPM could not be available in the SECURED context. We have assessed that the level of security of remote attestation solutions that use secure HW as root of trust is not reachable with software-only protections developed in ASPIRE. The only issue with HW-based RA is that the environment for a correct use of a TCG-based solution is too far from any possible use in the real world, despite any declaration of HW producers and their marketing departments. The software to perform the attestation in the SECURED infrastructure needs to be executed on machines that have a TPM. The SW-only remote attestation can only be considered for cloud-based solutions, where there is not a clear physical and its TPM. Moreover, we have also assessed that the remote attestation can be used to protect the SECURED app, the piece of software running on the user terminals in charge for communicating with the SECURED infrastructure and the user security application execution environments.

Nagravision participates to the Celtic-plus project (http://celticplus.eu/) on HEVC Hybrid Broadcast Video Services (H2B2VS, http://h2b2vs.epfl.ch). That project investigates the hybrid distribution of TV programs and services over heterogeneous networks. H2B2VS impacts requirements Nagravision puts forward for ASPIRE technology. Vice versa, ASPIRE uncovers options to securely deploy heterogeneous end devices as targeted by H2B2VS.e able to get connected, and where we will disseminate project results.

Section 8 List of Abbreviations

ACM	Association of Computing Machinery
ARO	Army Research Office
ASPIRE	Advanced Software Protection: Integration, Research and Exploitation
CARDIS	Smart Card Research and Advanced Application Conference
CC	Compiler Construction
CCS	Computer and Communications Security
CGO	Code Generation and Optimization
CHES	Cryptographic Hardware and Embedded Systems
CRYPTO	Cryptology
CSL	Computer Systems Lab
CSP	Cyber Security & Privacy
DAC	Design Automation Conference
DAPA	Digital Asset Protection Association
DATE	Design, Automation & Test in Europe
DoW	Description of Work
DRM	Digital Rights Management
ESORICS	European Symposium on Research in Computer Security
EU	European Union
EUROCRYPT	Annual International Conference on the Theory and Applications of Cryptographic Techniques
H2B2VS	HEVC Hybrid Broadcast Video Services
HiPEAC	High Performance and Embedded Architecture and Compilation
IEEE	Institute of Electrical and Electronics Engineers
ICSE	International Conference on Software Engineering
IT	Information Technology
LCTES	Languages, Compilers, Tools and Theory for Embedded Systems
NFC	Near Field Communication
NLL	Normandy Living Lab
PLDI	Programming Language Design and Implementation
RA	Remote Attestation
SECURED	SECURity at the network EDge
SIIA	Software & Information Industry Association
TACO	Transactions on Architecture and Code Optimization
TES	Secure Electronic Transactions (Transactions Electroniques Securisées in French)
TETRACOM	Technology Transfer in Computing Systems
TCG	Trusted Computing Group
TOPLAS	Transactions on Programming Languages and Systems
TORSEC	Torino Security
TPM	Trusted Platform Module
WP	Work Package